Practical Feasibility and Functional Safety of a Wheeled Mobile Driving Simulator

Vom Fachbereich Maschinenbau an der
Technischen Universität Darmstadt
zur Erlangung des Grades eines
Doktor-Ingenieurs (Dr.-Ing.)
genehmigte

Dissertation

vorgelegt von

Paul Wagner, M.Sc.
aus Weimar

Berichterstatter:	Prof. Dr. rer. nat. Hermann Winner
Mitberichterstatter:	Prof. Dr.-Ing. Günther Prokop
Tag der Einreichung:	05.04.2018
Tag der mündlichen Prüfung:	13.07.2018

Darmstadt 2018

Wagner, Paul: Practical Feasibility and Functional Safety of a Wheeled Mobile Driving Simulator
Darmstadt, Technische Universität Darmstadt,
Jahr der Veröffentlichung der Dissertation auf TUprints: 2018
URN: urn:nbn:de:tuda-tuprints-72966
Tag der mündlichen Prüfung: 13.07.2018

List of Contents

List of Abbreviations

Abbreviation	Description
ACL_{gain}	**A**cceleration **c**ue **l**atency calculated with $IACL_{gain}$
$ACL_{50\,\%}$	**A**cceleration **c**ue **l**atency calculated with $IACL_{50\,\%}$
BMS	**B**attery **m**anagement **s**ystem
C	**C**onsequence
COG	**C**entre **o**f **g**ravity
COS	**Co**ordinate **s**ystem
DiM	**D**river-**i**n-**m**otion
DOF	**D**egree **o**f **f**reedom
DS	**D**riving **s**imulator
E/E/PE	**E**lectrical/**e**lectronic/**p**rogrammable **e**lectronic
EM	**E**lectric **m**otor
EUC	**E**quipment **u**nder **c**ontrol
F	**F**requency of, and exposure time in the hazardous zone
FAS	**F**ahrer**a**ssistenz**s**ystem
FIR	**F**inite **i**mpulse **r**esponse filter
FKFS	Research institute of automotive engineering and vehicle engines Stuttgart (**F**orschungsinstitut für **K**raftfahrwesen und **F**ahrzeugmotoren **S**tuttgart)
FMEA	**F**ailure **m**ode(s) and **e**ffects **a**nalysis
FMECA	**F**ailure **m**ode(s), **e**ffects, and **c**riticality **a**nalysis
FS	**F**ahr**s**imulator
FTA	**F**ault **t**ree **a**nalysis
FZD	Institute of automotive engineering at Technische Universität Darmstadt (**F**ahr**z**eugtechnik **D**armstadt)
GB	**G**ear**b**ox
HAF	**H**och**a**utomatisiertes **F**ahren
HARA	**H**azard **a**nd **r**isk **a**nalysis
HMI	**H**uman-**m**achine-**i**nterface
HV	**H**igh **v**oltage (> 60 V (DC))
$IACL_{gain}$	**Gain**ing **i**ndicator for **a**cceleration **c**ue **l**atency
$IACL_{50\,\%}$	**50 % i**ndicator for **a**cceleration **c**ue **l**atency
IAD	Dresden institute of automobile engineering (**I**nstitut für **A**utomobiltechnik **D**resden)
IEC	**I**nternational **e**lectrotechnical **c**ommission
IMD	**I**nsulation **m**onitoring **d**evice
LP	**L**ow-**p**ass filter
LV	**L**ow **v**oltage (< 60 V (DC))
MC	**M**otion **c**ontrol

Abbreviation	Description
MCA	**M**otion **c**ueing **a**lgorithm
MORPHEUS	**M**obile **o**mnidi**r**ectional **p**latform for **h**ighly dynamic and tir**e**bo**u**nd driving **s**imulation
MSD	**M**ean **s**tandard **d**eviation
P	**P**ossibility of avoiding the hazardous event
PLC	**P**rogrammable **l**ogic **c**ontroller
PSA	**P**eugeot **s**ociété **a**nonyme
PSD	**P**ower **s**pectral **d**ensity
rtm	Department of control systems and mechatronics at Technische Universität Darmstadt (Fachgebiet **R**egelungs**t**echnik und **M**echatronik)
SaSy	**Sa**fety **sy**stem
SIL	**S**afety **i**ntegrity **l**evel
TC	**T**ilt **c**oordination
VeHIL	**Ve**hicle **h**ardware **i**n the **l**oop
VTI	Swedish national road and transport research institute (Statens **v**äg- och **t**ransportforsknings**i**nstitut)
W	**P**robability of the unwanted occurrence
WMDS	**W**heeled **m**obile **d**riving **s**imulator

List of Symbols and Indices

Symbol	Unit	Description
a	m/s²	Acceleration
b	m	Workspace
C	./.	Dimensionless tuning parameter
d	m, ./.	Displacement, dimensionless damping constant
e	./.	Dimensionless equivalency factor
E	J, Wh	Energy
f	Hz, ./.	Frequency, dimensionless coefficient
F	N	Force
g	m/s²	Gravitational constant (= 9.81 m/s²)
G	1	Transfer function
h	m	Height
I	A	Electric current
l	m	Length
m	kg	Mass
n	./.	Amount
P	W	Power
r	m	Radius
s	rad/s	Laplace (complex frequency) operator
t	s	Time
T	Nm	Torque
U	V	Electric voltage
v	m/s	Velocity
α	°	Slip angle
β	°	Tilt angle
δ	°	Steering angle
η	./.	Efficiency
θ	kgm²	Moment of inertia
μ	./.	Coefficient of friction
σ	./.	Standard deviation
τ	s	Time constant (e.g. feedback gain)
ψ	°	Yaw angle
ω	rad/s	Wheel speed
T	1/s	Inverted time constant

Index	Description
DS	Driving simulator(-fixed)
dyn	Dynamic
E	Earth-fixed
el	Electric
em	Energy model
hor	Horizontal
i	Count (from 1 to maximum)
I	Inertial
lat	Lateral
lim	Limitation
long	Longitudinal
nom	nominal
R	Resistance
sim	Simulation
t	Triangle
trans	Translational
V	Vehicle(-fixed)
W	Wheel(-fixed)
x	Surge DOF
y	Sway DOF
z	Heave DOF
θ	Pitch DOF
φ	Roll DOF
ψ	Yaw DOF

Kurzfassung

Der automobile Entwicklungsfokus verschiebt sich von der Entwicklung von Fahrerassistenzsystemen (FAS) hin zu (hoch-)automatisiertem Fahren (HAF), wie der Tagespresse entnommen werden kann. Dabei sind sich Experten einig, dass Fahrsimulatoren (FS) bei der Absicherung von HAF eine noch wichtigere Rolle zukommen wird, also schon bei FAS. Der Stand der Technik der FS befindet sich in Bezug auf die Wiedergabequalität von Beschleunigungen jedoch in einer Sackgasse, da die gestellten Dynamikanforderungen nicht ökonomisch erfüllt werden können, was die Validität der im FS erzielten Ergebnisse beeinträchtigt und somit ein bahnbrechendes, neues Konzept auf den Plan ruft.

Deshalb wird hier das Konzept eines selbstfahrenden Fahrsimulators (WMDS) untersucht, um bei mindestens gleichwertiger Immersion des Probanden und reduzierten Kosten den Stand der Technik zu ersetzen. Diese Arbeit beleuchtet das übergeordnete Projektziel des Machbarkeitsnachweises von WMDS unter zwei Gesichtspunkten: Ist die selbstfahrende Plattform praktisch in der Lage die gleiche Horizontaldynamik, wie sie in einem realen Fahrzeug auftritt, in Bezug auf Leistungsbedarf, Energiebedarf und Bewegungslatenz abzubilden, sowie welche Funktionen und Überwachungsmaßnahmen sind erforderlich, um das von einem WMDS ausgehende Risiko auf ein akzeptables Niveau zu reduzieren?

Die erste Forschungsfrage wird mittels Fahrversuchen mit dem skalierten WMDS-Prototyp MORPHEUS untersucht. Da aufgrund der begrenzten Fahrfläche für MORPHEUS keine unskalierten Stadtfahrmanöver durchführbar sind, wird ein Leistungs-/Energiemodell entwickelt, parametrisiert und validiert, mit dem ein unskalierter Energiebedarf sowie der Leistungsbedarf in Abhängigkeit des Skalierungsfaktors simuliert werden. Der Leistungs- und Energiebedarf sowie die Anforderungen an die Bewegungslatenz sind nachweislich mit dem Stand der Technik erfüllbar.

Die zweite Forschungsfrage wird untersucht, indem eine Gefahren- und Risikoanalyse durchgeführt wird und daraus Sicherheitsanforderungen abgeleitet werden. Eine Sicherheitsarchitektur wird entworfen, wobei ein autarkes Notbremssystem das Kernelement darstellt. Eine exemplarische Ausführung der Architektur wird auf die erreichte Risikoreduktion sowie auf neuerlich generierte Gefahren durch die dem System hinzugefügten Komponenten und Funktionen untersucht und weist nach, dass keine unakzeptablen Risiken mehr vorhanden sind.

Zusammenfassend liefert die vorliegende Dissertationsschrift den nächsten Baustein zum Machbarkeitsnachweis von WMDS und damit zur Revolution der FS-Technologie.

Short Summary

The automotive development focus shifts from advanced driver assistance systems towards automated driving, as can easily be concluded from daily news. While the validation and verification of driver assistance systems is already challenging, the question of how to validate automated driving is still unanswered. Nevertheless, it is widely agreed that the importance of Driving Simulators (DS) for the validation of driver assistance systems will increase even further for the validation of automated driving. Still, state-of-the-art DS are in a deadlock when it comes to providing the demanded quality in motion representation because larger workspaces are needed but cannot be provided economically, thus, impeding validity of DS results and calling for a ground-breaking concept.

A Wheeled Mobile DS (WMDS) is researched at FZD to replace state-of-the-art DS while providing an at least equal immersion to the test person with reduced costs. Therefore, this thesis investigates the superordinate project goal of proving feasibility of WMDS from two viewpoints: Firstly, is the wheeled motion base practically capable of providing the horizontal dynamics as they would occur in a real car in the aspects power demand, energy demand, and motion latency. Secondly, what measures are needed to reduce the risk that arises from the unbound system to an acceptable level and how are these measures triggered and monitored, ergo: How would a safety architecture need to look like for a WMDS?

The first research question is addressed by conducting driving manoeuvres with the scaled WMDS prototype MORPHEUS. As unscaled urban driving manoeuvres cannot be driven with MORPHEUS, since the available driving areas are not large enough, a power/energy model is developed, parameterised, and validated, enabling the simulation of the unscaled energy demand and of the power demand in dependence of the scaling factor. Concluding, the requirements to power and energy demand as well as motion latency can be fulfilled by state-of-the-art technology.

To answer the second research question, a state-of-the-art hazard and risk analysis has been conducted and safety requirements have been derived. An overall safety architecture is designed for these safety requirements, whereas the core element is an autarchic emergency braking system. An exemplary design of this safety architecture is investigated and evaluated in terms of risk reduction and additional hazards arising from the newly introduced functions and components, yielding that no unacceptable risk is inherited in the system.

Concluding, the herein presented work provides the next building block towards proving general feasibility of WMDS and, thus, towards revolutionising DS technology.

1 Introduction

1.1 Motivation

As already mentioned in the summary, the automotive development focus shifts from advanced driver assistance systems (SAE Level 0-2[1]) towards automated driving (SAE Level 3-5[1]) and the importance of Driving Simulators (DS) for the validation of advanced driver assistance systems[2,3,4,5,6] as well as of automated driving[7,8,9] is undisputed, especially for urban applications. Not to mention other areas of application that will remain relevant in near future such as driver behaviour analysis, Human-Machine Interface (HMI) development and validation, and dimensioning of chassis components[3,4,6,10]. This continuing interest in DS is due to its key advantages reproducibility, e.g. in studies involving many test subjects undergoing the same driving scenario, safety for the subject, e.g. when investigating safety critical driving manoeuvres such as an emergency evasion, and – of course – cost and time reduction in the development process due to the early availability of virtual prototypes.

When looking back at the historic development of DS, a trend towards more realistic – in terms of motion feedback – driving simulation becomes evident: In the late 1950s the first fixed-base DS were developed, succeeded by dynamic DS with Stewart platforms in the late 1960s. It was not until the end of the 20th century that highly dynamic DS were developed, employing xy-rails for a better representation of high frequent and/or sustaining

[1] SAE: Terms Related to Automated Driving Systems (2014).

[2] Zeeb, E.: Daimler's New Full-Scale, High-Dynamic DS (2010).

[3] Baumann, G. et al.: How to Build Europe's Largest Eight-Axes DS (2012).

[4] Blana, E.: A Survey of DS Around the World (1996). a: pp. 4-7.

[5] Chapron, T.; Colinot, J.-P.: The New PSA Advanced DS (2007).

[6] Schöner, H.-P.: Erprobung und Absicherung im dynamischen DS (2014).

[7] Richter, A.; Scholz, M.: The Surveyor's Guide to Automotive Simulation (2016).

[8] Boer, E. R. et al.: The Role of DS in Developing and Evaluating AD (2015).

[9] Maurer, M. et al.: Autonomes Fahren (2015). p. 446.

[10] Schöner, H.-P.; Morys, B.: Dynamische DS (2015). p. 140.

translational accelerations[11]. Many efforts were undertaken after that to increase the quality of the acceleration representation and therefore the immersion as well. However, large workspaces are required to provide the equal acceleration sensation as in a real car, with urban driving – which requires the highest developmental effort for automated driving – being the worst-case application scenario[12]. This dilemma was accurately summarised by Zeeb, former head of Daimler DS, in 2010: "To induce a much better longitudinal motion sensation with a scaling factor close to 1:1 for all possible acceleration and deceleration scenarios even a several ten meter long sledge would not be sufficient, but would increase the technical and financial effort tremendously, especially when the […] mandatory requirements for drive dynamic experiments have to be fulfilled"[13].

The prescribed controversy – the increasing importance of highly realistic DS for automotive research and development vs. the dynamic limitations of state-of-the-art highly dynamic DS – calls for a ground-breaking new concept. Thus, this work focuses on the advancement and proof of feasibility of the Wheeled Mobile Driving Simulator (WMDS) that is investigated by the Institute of Automotive Engineering (Fachgebiet Fahrzeugtechnik FZD) at Technische Universität Darmstadt since 2010.

1.2 Wheeled Mobile Driving Simulator Research at FZD

This section gives a brief overview of the WMDS research and its methodology at FZD. The herein described hypotheses are used throughout the entire project and will partially be investigated in this thesis. Thus, this section will enable the reader to rank the scientific merit of this thesis among FZD's overall WMDS research scope.

1.2.1 Overall Project Goal

Because setting up a WMDS is a tremendous effort – in economical and labour terms – the feasibility of the concept must be proven beforehand. Thus, the overall project goal is to demonstrate that FZD's WMDS concept can replace state-of-the-art DS with equal or higher immersion of the test person while costs are decreased compared to enhanced Stewart motion base DS (e.g. DS with compound slides). For being able to scientifically research feasibility, this overall project goal is stipulated as the main hypothesis H1:

[11] Blana, E.: A Survey of DS Around the World (1996).

[12] Betz, A. et al.: Motion Analysis of a WMDS (2012). pp. 5f.

[13] Zeeb, E.: Daimler's New Full-Scale, High-Dynamic DS (2010). p. 162.

H1: FZD's WMDS concept is able to provide equal or higher immersion to the test person while acquisition and maintenance costs are decreased compared to state-of-the-art enhanced Stewart motion base DS.

The hypothesis succeeds if all attempts of falsification fail. The soundest falsification test is to build a WMDS, evaluate the immersion in a representative study with test persons, and calculate the costs. Unfortunately, as initially described, the stakes for conducting this test are high and the outcome is uncertain. Therefore, criteria must be identified that bear the potential to falsify the main working hypothesis in theory and practical applications. Thus, the risk of bad investments is reduced. These criteria are referred to as *falsification aspects* and must be researched in worst-case scenarios so that no trivial verifications (e.g. comparing the high-fidelity WMDS concept with a low-fidelity DS) are conducted. If the aspects' investigations fail to falsify the hypothesis in theory or practical application, the concept is considered feasible.

1.2.2 Initial Situation

Previously conducted work at FZD, conducted by Betz[14], analysed the following five falsification aspects:

1. Power demand (theoretical)
2. Energy demand (theoretical)
3. Friction coefficient (practical application)
4. Motion control (theoretical)
5. Safety architecture (exemplary practical application of an emergency braking system)

Whereas the falsification aspects power and energy demand as well as motion control have been analysed theoretically in a virtual prototype (cf. section 5.2), the friction coefficient and the safety architecture were investigated with a hardware prototype that was designed and manufactured in the author's master's thesis[15] and is described in detail in chapter 3. While the aspect friction coefficient was not able to falsify the working hypothesis, the safety concept has only been exemplarily demonstrated by an emergency braking system integrated into the hardware prototype. Neither risk has been assessed, nor the triggering and fault monitoring mechanism has been set up. Thus, the falsification aspect of a safety architecture has not been sufficiently investigated, yet.

[14] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015).

[15] Wagner, P.: Master's thesis, Aufbau und Inbetriebnahme eines WMDS (2013).

1.2.3 Working Hypotheses

Besides Betz' five falsification aspects, two additional falsification aspects are identified, whereas the aspect of vertical dynamics is analysed by Zöller, who already published parts of his findings[16,17]:

6. Latency
7. Vertical dynamics

Concluding, the seven falsification aspects are transferred into working hypotheses that are derived from the main hypothesis and must be researched within the overall project scope. Again, this thesis covers neither all hypotheses nor all falsification aspects.

1.2.3.1 Wheeled Motion Base

The working hypothesis H1.1 is adapted from Betz and addresses the five falsification aspects power demand, energy demand, friction coefficient, motion control, and motion latency:

> H1.1: "The wheeled motion base of [FZD's] WMDS [concept] with its dynamics limited by friction forces can simulate the horizontal dynamics of urban traffic for normal driver behaviour considering common scaling factors"[18].

"The two restrictions of the hypothesis concerning *normal driver behaviour* and *common scaling factors* are stipulated because no effort is desired that causes higher requirements than necessary. First, the driving experience that is intended to be reproduced in the DS is limited in its dynamics due to the driving behaviour of normal drivers. In other words, no expert or race car drivers are considered, and the road traffic regulations are obeyed. Second, advantage is gained from the common scaling factors as they are found in literature because human perception may be fooled in certain ranges without causing disturbing losses in the perceived driving experience [(further details can be found in sections 2.1.4 to 2.1.6 and 2.5.2)]"[18].

1.2.3.2 Safety Architecture

Hypothesis H1.2 addresses the falsification aspect of a suitable safety architecture:

> H1.2: FZD's WMDS concept does not bear an unacceptable risk to a human under any environmental conditions and in any use case.

[16] Zöller, C. et al.: Tire Concept Investigation for WMDS (2016).

[17] Zöller, C. et al.: Tires and Vertical Dynamics of WMDS (2017).

[18] Cf. Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 4.

FZD's WMDS concept is characterised by its ability to move freely on a planar surface, which excludes stop dampers from being used, as it is currently done in highly dynamic DS. An *unacceptable risk* is context-dependent and is "judged to be unacceptable [..] according to valid societal moral concepts"[19]. For technical systems, various approaches exist that evaluate the risk based on risk parameters determined in a thorough analysis (section 2.3). Thus, the WMDS and its safety architecture must comply with state-of-the-art norms (e.g. IEC 61508) and guidelines (e.g. VDI 2221). *Humans* interacting with the WMDS must be considered in the design of the safety architecture. Hypothesis H1.2 includes the operation and maintenance of the WMDS and, therefore, subjects such as test persons, maintenance personnel, and bystanders.

1.2.3.3 Vertical Dynamics

Hypothesis H1.3 addresses the falsification aspect of the vertical dynamics excitation resulting from the tire road contact:

> H1.3: FZD's WMDS concept can simulate urban driving scenarios on any driving surface, which is commonly driven on with WMDS, without impairing the test person's immersion.

C*ommon driving surfaces for the application of WMDS* must be defined because the concept is unprecedented worldwide. Potential users of WMDS can help by considering on which surfaces they would use a WMDS. In this hypothesis' context, the *immersion* refers to vertical excitations that do not disturb the overall driving experience of the test person. Values can be found in literature or in experiments.

1.3 Overall Methodology and Structure of the Thesis

This thesis researches the falsification aspects of practical power demand, energy demand, and latency of hypothesis H1.1 and the theoretical falsification aspect of a safety architecture, hypothesis H1.2. The aim is to identify the worst-case for each aspect under the given constraints (e.g. normal driver behaviour) and with state-of-the-art technology to conduct a most rigorous falsification.

[19] ISO TC 22/SC 32 Electrical and electronic components and general system aspects: ISO 26262 (2011). p. 18.

1.3.1 Wheeled Motion Base

The research questions that are investigated for the falsification of hypothesis H1.1 are:

1. Power demand: Is FZD's WMDS concept capable of providing the maximum power demanded with state-of-the-art components (actuators, on-board power supply systems, tires, suspension, etc.)?
2. Energy demand: Are state-of-the-art on-board energy storage systems capable of providing the energy required for driving simulation as described by hypothesis H1.1?
3. Latency: Which motion latency from the driver's input to the provided acceleration cue must be undercut and is FZD's WMDS concept capable of providing cues within this latency in order to represent the same motion sensation as in standard passenger cars?

Sections 2.4 to 2.5 describe the state-of-the-art of accumulators and human motion perception. This knowledge allows to extrapolate from the capabilities of the hardware prototype to what can be achieved, defining the worst-case requirements and constraints for the experiments (sections 4.1 to 4.3, in which the detailed methodology with the experimental setup and evaluation criteria can be found). A bottom-up methodology is applied for identifying the worst-case power demand, energy demand, and latency of FZD's WMDS concept. The investigation is done with real driving of the hardware prototype, starting from simple manoeuvres evolving into more complex manoeuvres, section 5.1. Because not all falsification experiments can be conducted on a 1:1 scale, the investigation is supported by a virtual prototype, section 5.2. If the required outputs of the virtual prototype are validated with the hardware prototype, the simulation results can be extrapolated, section 6. If these aspects cannot be falsified, they are practically feasible.

1.3.2 Safety Architecture

For the falsification of hypothesis H1.2, the worst-case risks any human is exposed to in all possible use cases, as defined in hypothesis H1.1, must be determined. Then, the research question is if these risks can be reduced to an acceptable level by a safety architecture. Relevant functional safety standards are described in section 2.3. The safety architecture itself is deduced from a top-down methodology. This implies that the safety architecture development is started by identifying all hazards (section 7.1.2, methodology section 4.4.2). Based on the identified hazards, risk is assessed (sections 7.1.3 and 7.2, methodology sections 4.4.3 and 4.4.4). All hazards with significant risk are included in a safety requirement list and a safety architecture design per state-of-the-art norms and guidelines (section 2.3) is proposed (section 7.3). The risk reduction as well as new hazards introduced to the system are evaluated for an exemplary application (section 7.3.3). Finally, an outlook to a safety architecture for full-scale WMDS is given (section 7.4).

2 State-of-the-Art and Scientific Research

This chapter starts with clarifying the used DS specific terminology (section 2.1, compatible with Betz'[20] definitions), followed by a brief overview of different types of DS with a detailed description of wheeled mobile DS (section 2.2). Finally, the required basic information (i.e. requirements) for investigating the falsification aspects safety architecture (section 2.3), energy demand (section 2.4), and latency (section 2.5) is addressed.

2.1 Definitions

2.1.1 Coordinate System (COS)

The Coordinate System (COS) is chosen per DIN ISO 8855[21a], where the index E represents the earth-fixed COS and V represents the vehicle's (in this context virtual vehicle) COS. Additionally, in this work the indices DS for the DS' COS and W for the wheel's COS are introduced. The translational Degrees Of Freedom (DOF) are denominated x for surge, y for sway, and z for heave. The rotational DOF are denominated θ for pitch, φ for roll, and ψ for yaw.

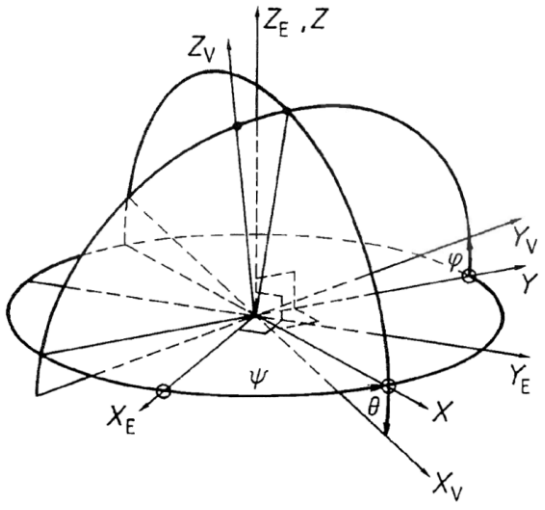

Figure 2-1: COS per DIN ISO 8855[21b]

[20] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). pp. 9-12.

[21] Deutsches Institut für Normung e. V.: ISO 8855 (2013). a: - ; b: p. 11.

2.1.2 Simulator Orientation

The x-direction of the DS (x_{DS}) is the direction the test person's seat is facing. According to DIN ISO 8855[22], the lateral direction (y_{DS}) is positive to the left and the vertical direction (z_{DS}) upwards. The steering and drive units are numbered (1 to 3) clockwise, starting at the unit faced by the test person's seat, cf. Figure 2-2:

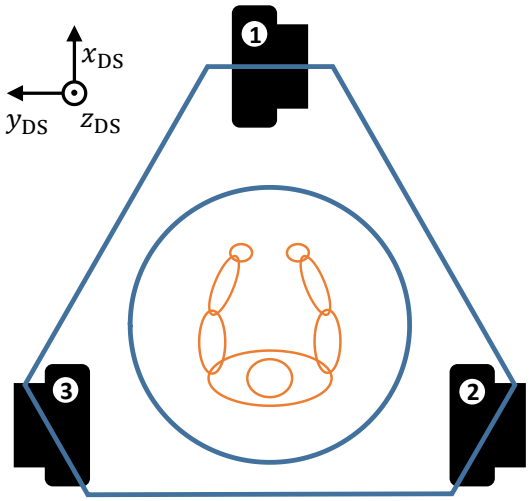

Figure 2-2: DS orientation

2.1.3 Motion Cue / Motion Cueing Algorithm (MCA)

Synonyms for the term *cue* are reference, indication, or information. When working with humans, this term is commonly used for describing a sensory information that is provided[23,24]. Therefore, the term *motion cue* describes a sensory information that is perceived and interpreted by the test person as motion. Because motion is primarily perceived through the vestibular sensory organ (cf. section 2.5.1), the term *motion cue* is used within this thesis for describing a vestibular stimulus that is presented to the subject. The algorithm that translates motion cues of a real car into the motion cues of the DS is referred to as the Motion Cueing Algorithm (MCA).

2.1.4 Scaling

Scaling describes the process of proportionally reducing the acceleration amplitudes within a DS, e.g. when the acceleration amplitude of 4 m/s² of a real car is to be simulated

[22] Deutsches Institut für Normung e. V.: ISO 8855 (2013).

[23] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 10.

[24] Fischer, M.: Diss., MCA für eine realitätsnahe Bewegungssimulation (2009). p. 5.

in a DS with a scaling factor of 0.5, the simulated DS acceleration would be 2 m/s². Scaling reduces the amplitude uniformly across all frequencies[25a] and not necessarily impedes the subject's immersion[26]. Commonly used scaling factors are 1, 0.7, and 0.5, depending on the manoeuvre that is to be simulated and on available workspace limiting the acceleration amplitude in dependence on the acceleration frequency[26,27a,28]. As stated by Betz[29], it is not clear whether the yaw motion should be scaled as well. On the one hand scaling the yaw motion would match the scaled lateral acceleration, on the other hand the unscaled visual cues would contradict the scaled yaw motion. Therefore, an unscaled yaw motion is used here, resulting in a conservative investigation of WMDS.

2.1.5 Tilt Coordination (TC)

Tilt Coordination (TC) basically describes a measurement error that can occur with humans and sensors if perception is based on the measurement of inertia forces. If the sensor (vestibular organ for a human) is tilted relative to the gravitational force vector, the sine portion of the gravitational force is perceived as horizontal acceleration[25b,27b,29]. This phenomenon is applicable up to certain ranges of tilt angles, tilt rates, and tilt accelerations, often described as stationary perception thresholds (section 2.5.2). Nevertheless, this technique is predestined for application in DS since almost all dynamic DS use motion systems with six DOF or more that can tilt the subject. Thus, low frequent accelerations may be well presented through TC. The frequencies are partitioned by the MCA. The delusion may be perceived by the subject if the vestibular channel does not match the cues from other sensory channels. Therefore, especially visual cues must adapt to TC.

2.1.6 Washout

The *washout* aims at minimising the required workspace. This is achieved by moving the DS back into its initial position below human perception thresholds or by masking the washout motion with TC[27b]. Usually this is done filter-based within the MCA, therefore, the term washout is also often used for referring to the (classical) MCA[25c,30].

---

[25] Reid, L. D.; Nahon, M.: Flight Simulation MCA (1985). a: Appendix B.1; b: 1.1; c: - .

[26] Greenberg, J. et al.: Lateral Motion Cues During Simulated Driving (2003).

[27] Fischer, M.: Diss., MCA für eine realitätsnahe Bewegungssimulation (2009). a: pp. 57f.; b: pp. 6f.

[28] Groen, E. et al.: Psychophysical Thresholds of Linear Acceleration (2000).

[29] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 11.

[30] Nahon, M.; Reid, L. D.: Simulator MCA - A Designer's Perspective (1990).

2.1.7 Simulator Sickness

Simulator sickness must be avoided in driving simulation experiments and refers to an illness-like condition whose symptoms can be nausea, vomiting, cold sweating, and pallor. The most widely accepted theory behind simulator sickness is the sensory conflict theory[31], according to which simulator sickness occurs if the cues perceived by the vestibular receptors, the eyes, or the non-vestibular proprioceptors mismatch. Reason and Brand[31] divide simulator sickness into two classes: The first class is caused by mismatching cues between the eyes and vestibular receptors, whereas the second class is caused by mismatching cues between the semi-circular canals and the otoliths within the vestibular organ (cf. section 2.5.1). While the second class is mainly influenced by a properly tuned MCA, the first class is influenced by delayed or missing representation of one of the aforementioned cues[32]. Whereas completely missing cues can be system inherent if an insufficient or no motion system at all is used in the DS, simulator sickness induced by delayed cues is caused by latency in either the visual representation system or the motion system. These delayed cues are primary responsible for simulator sickness according to literature[33]. Latency is dealt with in more detail in section 2.5.3.

2.2 State-of-the-Art Driving Simulators

The motion capabilities of DS have changed dramatically in the latter half of the 20th century but did not improve much since then. This section gives a brief overview of these motion capabilities and corresponding areas of application. The DS are ranked in the order of increasing motion capability. The exemplary designs that are chosen represent top of the class DS in terms of available acceleration amplitude and sustained acceleration. A more in-depth analysis has been conducted by Schöner and Morys[34] or more complete analyses by Blana[35] or Slob[36].

---

[31] Reason, J. T.; Brand, J. J.: Motion Sickness (1975).

[32] Hettinger, L. J.; Riccio, G. E.: Visually Induced Motion Sickness (1992). p. 306.

[33] St. Pierre, M. E.: Diss., The Effects of Latency on Simulator Sickness in a HMD (2012). pp. 16-18.

[34] Schöner, H.-P.; Morys, B.: Dynamische DS (2015).

[35] Blana, E.: A Survey of DS Around the World (1996).

[36] Slob, J. J.: State-of-the-Art DS (2008).

2.2.1 Fixed Base DS

Fixed base simulators origin back to early flight simulators in the beginning of the 20th century, inheriting the very basic element of a simulator: The HMI. DS in the 1960s already showed visual representation, audition was represented by the 1970s[37]. Therefore, visual and audible feedback constitute the second and third basic elements of a DS.

2.2.2 Stewart Motion Base DS

A Stewart Platform – based on the universal tyre test machine by Gough[38] – consists of two platforms that are connected by six linear actuators[39] and is nowadays usually referred to as *hexapod*. The setup allows motion in all six translational and rotational DOF. Applied to a fixed base DS, the test subject can be moved, which results in an increased immersion and, therewith, motion cues constitute the fourth basic element of a DS. However, due to the limited stroke of the actuators and in dependence on the acceleration amplitude, only short acceleration cues can be represented. More advantageous, the rotational DOF allow to tilt the test subject and, therefore, enable TC with sustaining acceleration cues but limited frequency.

2.2.3 “Robocoaster” Motion Base DS

The Robocoaster motion base DS is based on the Robocoaster robot arm for entertainment purposes that in turn is based on a KUKA robot arm for industrial purposes[40]. The use of a robot arm increases the available motion compared to a hexapod and therewith also the immersion of the test subject. Nevertheless, accelerations still cannot be represented for all frequencies and amplitudes that occur while driving a car. Advantageous – compared to Stewart motion bases – is the increased yaw angle. The Max Planck Institute for Biological Cybernetics extended its Robocoaster by a linear track that adds 9.88 m of motion envelope[41]. This adds to the immersion but still limits the DS in its capabilities to represent sustaining high amplitude accelerations. Further disadvantages of the concept are the complex control and safety architecture.

---

[37] Blana, E.: A Survey of DS Around the World (1996). pp. 4-7.

[38] Gough, V. E.; Whitehall, S. G.: Universal Tyre Test Machine (1962).

[39] Stewart, D.: A Platform with Six DOF (1965).

[40] Teufel, H. et al.: MPI Motion Simulator (2007).

[41] Nieuwenhuizen, F. M.; Bülthoff, H. H.: The MPI CyberMotion Simulator (2013). p. 124.

2.2.4 Centrifuge Motion Base DS

Desdemona Ltd. developed the Desdemona simulator based on a centrifuge. The complex design allows translational motion as a hexapod, whereas rotational motion is possible up to over 360°[42]. Combined translational and rotational motion can create sustaining acceleration cues with high amplitudes. Nevertheless, also unwanted acceleration cues are generated, especially when initialising or ending a manoeuvre with sustained acceleration: The DOF are interdependent, which makes the control – in terms of the MCA – complex.

2.2.5 Cable Robot DS

In 2015, the Max Planck Institute for Biological Cybernetics introduced their cable robot DS. This DS is suspended by eight cables, each driven by an individual electric motor, enabling the usage of the entire room (5 x 8 x 5 m^3)[43]. Advantageous are the light concept and high acceleration amplitudes. Disadvantageous are elasticities of the cables that can result in vibration or latency in acceleration representation. Furthermore, to represent sustained high amplitude acceleration, the room and with that the length of the cables must be increased, worsening the elasticity issue. These disadvantages impede the use of cable robots for (nearly) unscaled high-fidelity driving simulation.

2.2.6 Enhanced Stewart Motion Base DS

Today's high-fidelity DS still employ a hexapod that is either carried on compound slides or by air cushions enhanced by further actuators. For the air cushion solution, linear actuators are used that connect to the hexapod motion base. Compound slide solutions may also use rotary actuators. Whereas the hexapod is used for TC and rotational movement of the car, the additional actuators are used to represent high frequency accelerations, i.e. accelerations that cannot be represented by TC due to the human motion perception thresholds (see section 2.1.5 and 2.5.2). Of course, adding a slide increases the weight of the DS significantly and, even worse, adding a crossbeam for the second slide exponentiates this issue since the first slide(s) must be moved together with the hexapod, cabin, etc. Power and energy demand are affected by the weight increase, too. Therefore, a natural trade-off between DS fidelity and economy seems to be given, as confirmed by Zeeb[44] (citation section 1.1). For comparatively smaller solutions, the hexapod can be carried by air cushions instead of slides, which reduces the moving mass. For spanning

[42] Wentink, M. et al.: Design and Evaluation of MCA for Desdemona Simulator (2005). p. 2.

[43] Max Planck Institute for Biological Cybernetics: CableRobot with Passenger (2015).

[44] Zeeb, E.: Daimler's New Full-Scale, High-Dynamic DS (2010). p. 162.

large workspaces, the stiffness of the actuators' pistons becomes critical. Nevertheless, more and more enhanced Stewart motion base DS are built around the world as can be seen in the selection of Table 2.1, proving the persistent demand of highly dynamic DS:

Table 2.1: Overview of enhanced Stewart motion base DS

Organisation	Motion envelope	DOF	Moving mass
Peugeot Société Anonyme (PSA)[45]	10 m x 5.5 m	8 DOF	unknown
Renault ULTIMATE[46]	6 m x 6 m	8 DOF	unknown
Swedish National Road and Transport Research Institute (VTI) Sim IV[47]	2.5 m x 2.3 m	8 DOF	unknown
University of Iowa[48]	20 m x 20 m	13 DOF	80 t
University of Leeds[49]	5 m x 5 m	8 DOF	unknown
Toyota[50]	35 m x 20 m	12 DOF	80 t[51]
Daimler[51]	12.5 m	7 DOF	unknown
Research Institute of Automotive Engineering and Vehicle Engines Stuttgart (FKFS)[52]	10 m x 7 m	8 DOF	unknown
VI-grade Driver-in-Motion (DiM) 250[53]; in application, inter alia, at Honda[54], Danisi Engineering[53], Volvo[53], Lamborghini[53], Porsche[53]	1.6 m x 1.5 m	9 DOF	unknown

2.2.7 Summary of State-of-the-Art DS

For proving that state-of-the-art DS are not capable of representing a sufficient acceleration sensation as it could be perceived when driving in a real car in an urban environment, the calculation of the frequency gaps between the tilt and translation mechanisms is

[45] Chapron, T.; Colinot, J.-P.: The New PSA Advanced DS (2007).

[46] Dagdelen, M. et al.: MPC based MCA (2004). p. 228.

[47] VTI: VTI's simulator facilities.

[48] Clark et al.: NADS Motion System (2001).

[49] University of Leeds: University of Leeds DS (2016).

[50] Murano, T. et al.: Development of High-Performance DS (2009).

[51] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 29.

[52] Baumann, G. et al.: The New DS of Stuttgart University (2012).

[53] VI-grade: VI-grade DiM (2017).

[54] Honda Deutschland: Honda R&D DS (2017).

stressed[55]: It is assumed that a longitudinal, harmonic excitation with an amplitude $|\hat{a}|$ of 5 m/s² is to be presented. The translation system is then limited by the available workspace, resulting in the lower limit frequency for translation, where $2b$ is the available workspace:

$$f_{\text{trans,lim}} > \frac{1}{2\pi}\sqrt{\frac{|\hat{a}|}{b}} \tag{2-1}$$

The tilt system (namely the hexapod) is then limited by the tilt rate threshold $\dot{\beta}_{\text{threshold}}$, resulting in the upper limit frequency for tilting:

$$f_{\text{tilt,lim}} \lesssim \frac{1}{2\pi}\frac{g}{|\hat{a}|}\dot{\beta}_{\text{threshold}} \tag{2-2}$$

To be able to represent the acceleration demand, the lower limit frequency for the translation system must meet the upper limit frequency for the tilt system. Obviously, the human perception threshold for tilt rate cannot be changed. Therefore, if scaling is left out, the only available parameter to be changed is the workspace b, yielding for $f_{\text{trans,lim}} = f_{\text{tilt,lim}}$

$$b = \frac{|\hat{a}|^3}{g^2\dot{\beta}_{\text{threshold}}^2} \tag{2-3}$$

Applying the tilt rate threshold that is used throughout the project of 6 °/s yields (section 2.5.2), whereas the workspace must be provided for acceleration and deceleration as well, yields:

$$b(\dot{\beta}_{\text{threshold}} = 6\,\frac{^\circ}{\text{s}}, |\hat{a}| = 5\,\frac{\text{m}}{\text{s}^2}) = \pm 118.4\text{ m} \tag{2-4}$$

It can be clearly seen that a workspace of ±118.4 m is economically impossible to achieve with a compound slides motion base DS[56]. Tüschen comes to a similar result of ±161 m, using a more restrictive tilt rate threshold of 5 °/s[57]. Figure 2-3 illustrates the frequency gaps that cannot be represented in dependence on the available translational workspace. The only reasonable approach to overcome this dilemma is an unbound system limited only by the environment it is moving in.

[55] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). pp. 20-23, 125.

[56] This value differs from the workspace calculated by Betz, who – inconsistently – used the tilt rate threshold of 3 °/s for the calculation of the frequency gaps instead of 6 °/s that were used throughout the rest of his thesis.

[57] Tüschen, T. et al.: Suspensions Design of a WMDS (2016). p. 6.

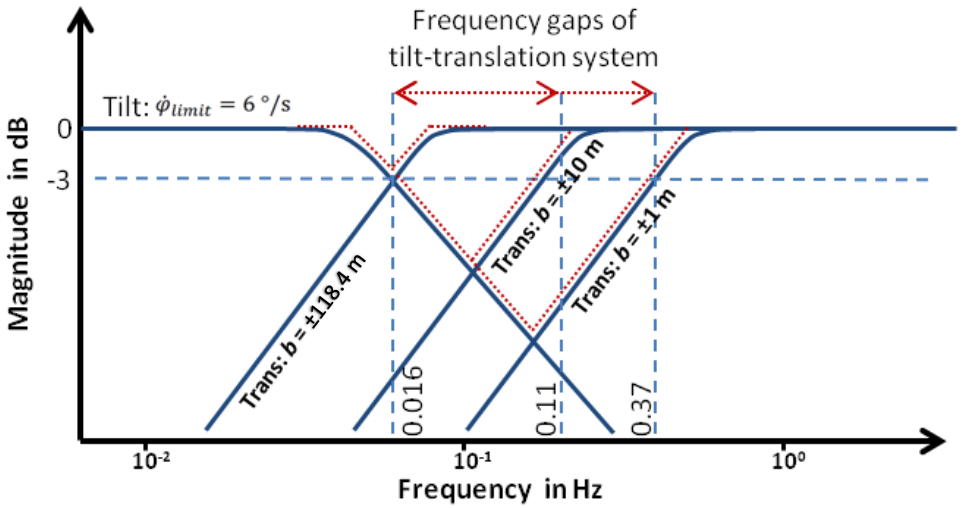

Figure 2-3: Frequency gaps of state-of-the-art DS (Hexapod ±1 m, compound slides motion base DS ±10 m, unrestricted ±118.4 m)[58]

2.2.8 State-of-Research: Wheeled Motion Base DS

2.2.8.1 BMW Patent

The first concepts of a wheeled motion base for DS were patented by Donges/BMW in 2002[59a] respectively Hüsing/BMW in 2003[60]. Their concept proposes an at least three-wheeled platform topped by a dome, in which a complete car or mock-up can be fitted. The wheel units may consist of single or twin wheels. The steering angle is limited to ±180°. Energy is supplied by a cable suspended from the ceiling, cf. Figure 2-4:

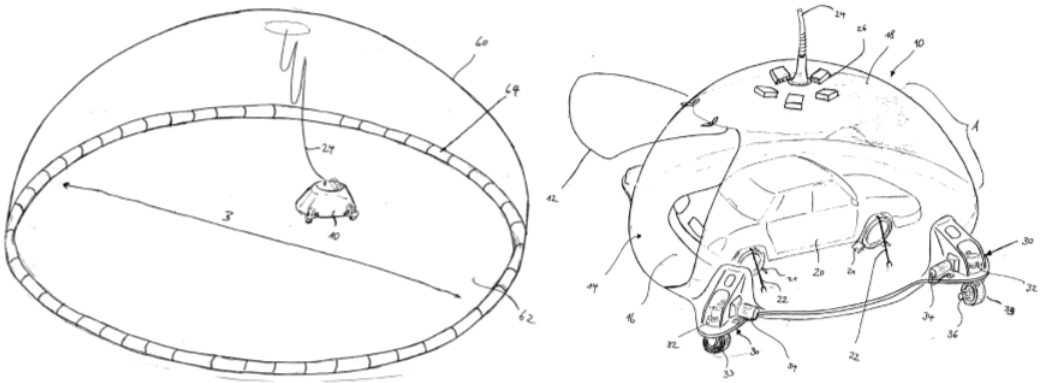

Figure 2-4: BMW wheeled motion base DS[59b]

[58] Cf. Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 22.

[59] Donges, E.: Fahrsimulator (2001). a: - ; b: pp. 6f.

[60] Hüsing, K.: Fahrsimulator (2001).

The safety architecture is described as an infrastructural element that obstructs the movement of the DS as soon as the workspace is left. Betz[61] described the drawbacks of BMW's concept. Firstly, it is unclear why the steering angle is limited to ±180°. Because the cabin's yaw angle and the DS' trajectory are dependent on each other, the limitation of the steering angle reduces the capabilities of the washout algorithm that drives the DS back into its initial position. Furthermore, the described safety architecture bears a significant infrastructural effort, because the whole workspace must be framed, and the safety infrastructure must cope with any impact speed and angle of the DS. Also, when it comes to mobile applications, e.g. on outdoor testing grounds, an infrastructural safety architecture is unsuitable.

2.2.8.2 Eindhoven University of Technology/Bosch Rexroth[62a]

The Eindhoven University of Technology researched together with Bosch Rexroth a 24-wheeled motion base DS whose wheels are grouped into four wheel carriers consisting of three twin wheels each. Solid tires are used. The dome can carry a complete vehicle and can be tilted, pitched, and heaved by a three-crank mechanism. Energy is supplied via a cable that is suspended from the ceiling.

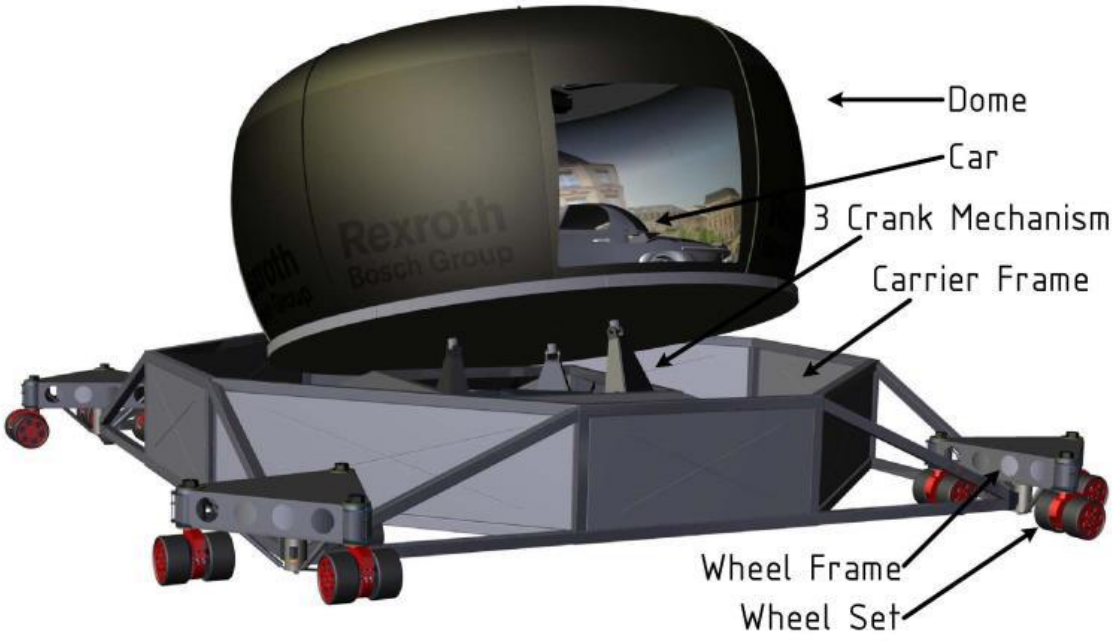

Figure 2-5: Wheeled motion base DS of Slob et al.[62b]

The publication is mainly focused on the wheel kinematics with the aim of representing acceleration cues instantaneously. Therefore, caster is used at each wheel set, Figure 2-6.

[61] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 39.

[62] Slob, J. J. et al.: The Wall is the Limit (2009). a: - ; b: p. 299.

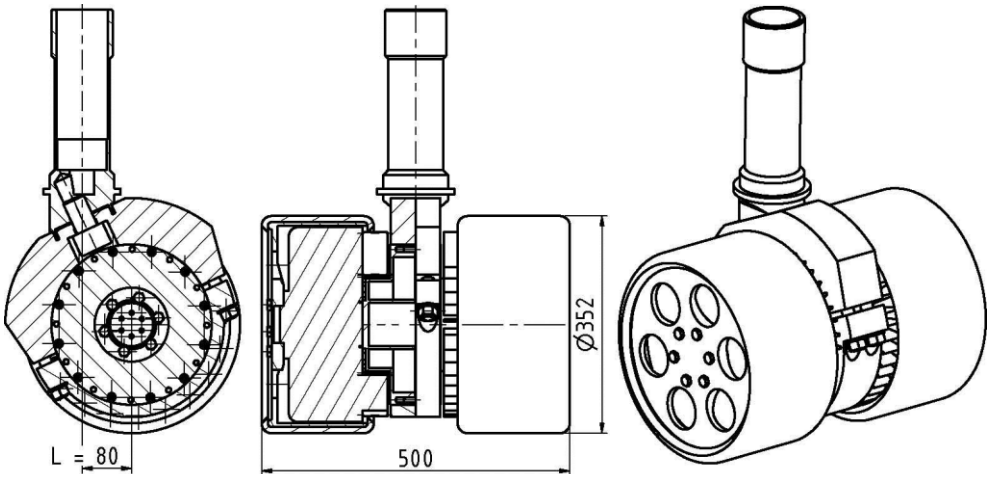

Figure 2-6: Wheel set design of Slob et al.[63a]

Longitudinal acceleration is generated by rotating the two wheels of a wheel set equally. In case of counterrotating those two wheels, a reaction torque is generated around point *A* (theoretical axis of rotation without caster, Figure 2-7). When a sufficient support torque around point *A* is provided, a lateral force at point *P* (wheel set's axis of rotation, Figure 2-7) is generated, resulting in instantaneous lateral acceleration.

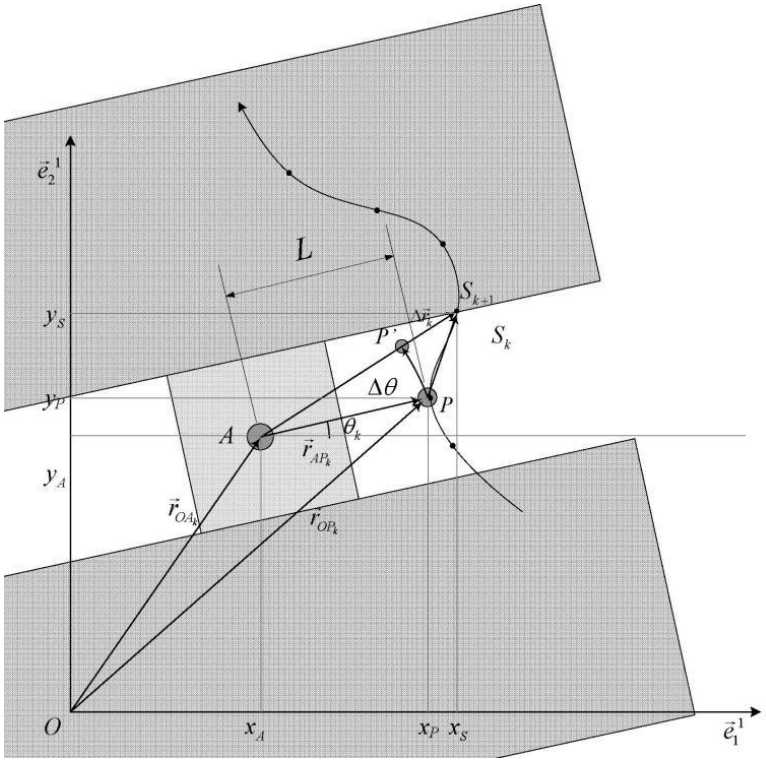

Figure 2-7: Wheel set kinematics of Slob et al.[63b]

[63] Slob, J. J. et al.: The Wall is the Limit (2009). a: p. 299; b: p. 301.

In theory, this concept can provide accelerations up to 7 m/s², Table 2.2, wherein the calculated overall weight of the DS is 11.1 t.[64a]

Table 2.2: Motion capabilities of wheeled motion base of Slob et al.[64b]

Non-simultaneous	Acceleration	Velocity	Displacement
Surge (x)	±7 m/s²	±4 m/s	± wall
Sway (y)	±7 m/s²	±4 m/s	± wall
Heave (z)	±5 m/s²	±0.4 m/s	±0.2 m
Roll (θ)	±5.2 rad/s²	±0.7 rad/s	±0.4 rad
Pitch (φ)	±5.2 rad/s²	±0.7 rad/s	±0.4 rad
Yaw (ψ)	±1.4 rad/s²	±1.1 rad/s	±1.2 rad

The safety architecture of this concept is not addressed within the paper, only the need for a positioning system is formulated. For control, an inverse kinematic algorithm is set up, neglecting nonlinearities of the tire behaviour.

One disadvantage of this concept is the energy supply via cable because mobile applications become impossible (as with the BMW patents). Furthermore, the paper aims at controlling the DS' trajectory, whereas the representation of acceleration is crucial for driving simulation. This is because humans are not able to perceive translational velocity directly (cf. section 2.5.1). The wheel caster approach overcomes the disadvantages of nonholonomic wheels, as Betz[65] already stated. Nevertheless, this problem occurs only in standstill. With moving wheels, lateral forces may be generated at any time. The paper does not address if the additional control effort with wheel caster weighs up the nonholonomic constraint of conventional wheels. Also, the nonlinear tire characteristic as well as cross influences through horizontal wheel forces, wheel load, and steering torque are not considered.

2.2.8.3 TNO VeHIL[66,67,68]

The Vehicle Hardware In the Loop (VeHIL) is a self-propelled platform used by TNO for evaluating vehicle sensors and their data processing as well as advanced driver assistance systems and automated driving. The test setup includes a chassis dynamometer on which

[64] Slob, J. J. et al.: The Wall is the Limit (2009). a: p. 306; b: p. 298.

[65] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 42.

[66] Gietelink, O. et al.: VEHIL: A Test Facility for ADAS (2004).

[67] van der Meulen, S. H.: Validation of Moving Base Simulation Model (2004).

[68] Ploeg, J. et al.: High Performance Automatic Guided Vehicle (2002).

the vehicle under test is mounted, so that it is stationary in the earth-fixed COS. Then the VeHIL platform, representing a vehicle within the trajectory of the vehicle under test, performs the inverted relative motion between those two vehicles. The wheels of the VeHIL platform are independently steerable, enabling omnidirectional movement. For positioning, odometry as well as a magnet grid integrated into the hall floor in combination with four linear antennas ("rulers" on the outside bottom edges of VeHIL, Figure 2-8) are used[69]. The accumulator allows for a 15-minutes test drive[70]. The technical specifications of the VeHIL platform are listed in Table 2.3:

Table 2.3: Technical specifications of TNO VeHIL platform[70]

Property	**Unit**	**Value**
Mass	kg	450
Maximum speed	km/h	50
Maximum acceleration	m/s²	10
Maximum steering angle	°	±350
Accumulator	./.	288 NiMH D-cells, 346 V (DC), 2.2 kWh

Figure 2-8: TNO VeHIL and the vehicle under test (background)[71]

The main difference between the TNO VeHIL platform and DS is that no subject is involved. This might explain why no references to the safety architecture of the platform can be found. In addition, the use of velocities and positions in the control architecture rather than accelerations results from the different application. Nevertheless, the VeHIL platform's horizontal motion behaviour is quite like that of wheeled motion base DS, whereas vertical excitation plays a minor role when compared with DS where ideally no

[69] van der Meulen, S. H.: Validation of Moving Base Simulation Model (2004). p. 13.

[70] Ploeg, J. et al.: High Performance Automatic Guided Vehicle (2002). p. 128.

[71] TU Delft: Validation Methodology for Fault-Tolerant ADAS (2014).

(non-artificial) road excitation must be perceived by the subject. Also, the concept proves that even accumulator technology from the year 2004 is an adequate energy supply for wheeled motion platforms.

2.2.8.4 Technische Universität Dresden/AMST-Systemtechnik GmbH

The Dresden institute of automobile engineering (Institut für Automobiltechnik Dresden, IAD) at Technische Universität Dresden started their wheeled motion base DS research in 2012 together with AMST-Systemtechnik GmbH. The main conceptual difference to the concept as investigated by FZD of Technische Universität Darmstadt is the use of four twin wheels instead of three single wheels and the use of a yaw turntable (ring bearing), cf. Figure 2-9. The simulator is powered by an on-board accumulator with the aim of mobile applications. Instead of a real car, a simplified and generic mock-up is used[72,73].

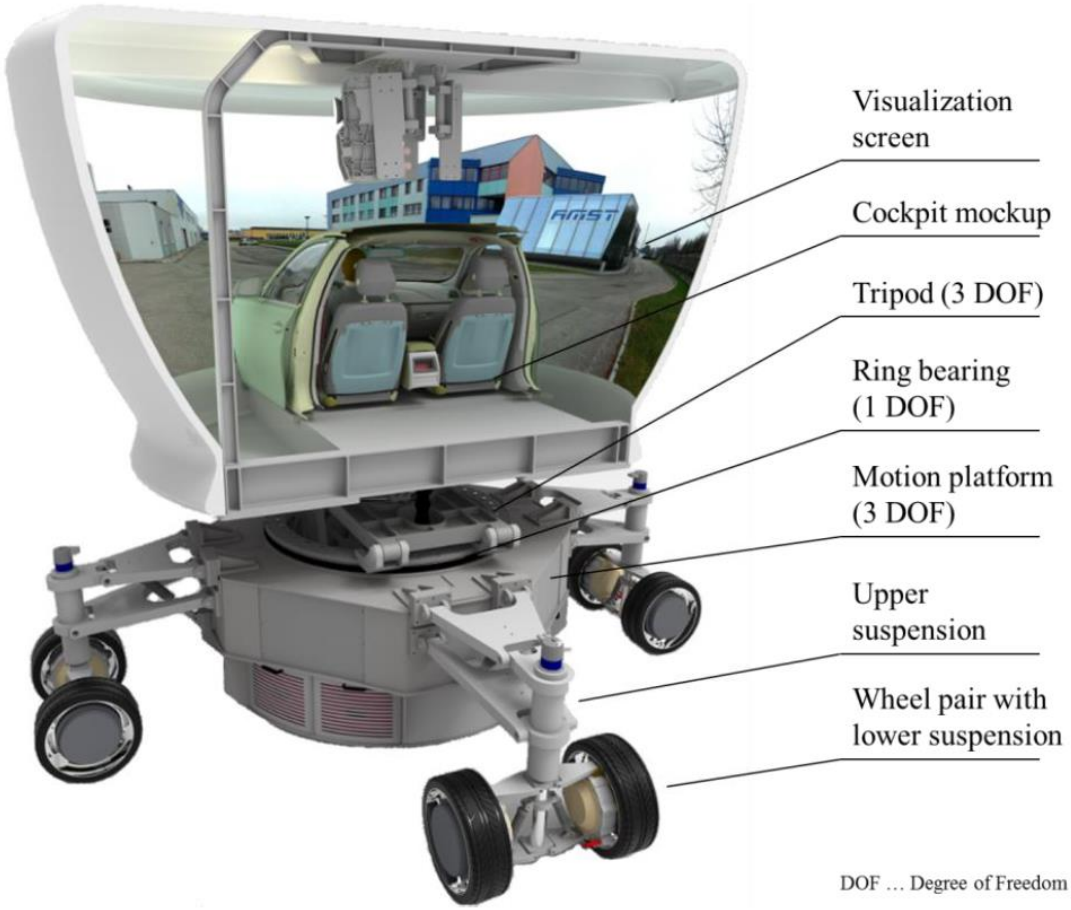

Figure 2-9: IAD's wheeled motion base DS[74]

[72] Tüschen, T.; Prokop, G.: Development of a Highly Dynamic DS (2013).

[73] Tüschen, T.: Diplomarbeit, MCA für einen WMDS (2013). pp. 9-12.

[74] Tüschen, T. et al.: Suspensions Design of a WMDS (2016). p. 9.

The yaw turntable constitutes a redundant DOF because the motion platform itself is also capable of yawing. To overcome the limitation of the non-holonomic constraint of the tire, the motion platform is constantly rotating while the dome is counterrotating. Thus, the subject will not notice the platform's rotation[75a]. The idea is that the wheels will never get into standstill so that lateral forces may be built up anytime. This is important because – without camber – tires build up lateral forces through generating a slip angle, which on the other hand means that the wheel needs to have a velocity vector that can be rotated. Nevertheless, none of Technische Universität Dresden's publications addresses how to avoid situations where the superposed rotation of the motion platform is cancelled out by the primary trajectory of the motion platform that is generated by the MCA. The likelihood of this event happening at one wheel is not negligible but becomes insignificant to happen for more than one wheel simultaneously[76]. Still, cancelling out the superposed rotation can lead to undesired motion cue latency and, therefore, false cues.

Another difference is the Motion Control (MC). Because the concept uses four sets of twin wheels, no explicit solution for calculating wheel loads and therewith horizontal target wheel forces exists. Therefore, the MC uses an inverted two-track vehicle model. From the two-track model, potential wheel forces are derived and handed over to an inverted tire model, where the wheel hub torques are calculated from Pacejka's magic formula[75b,77], Figure 2-10.

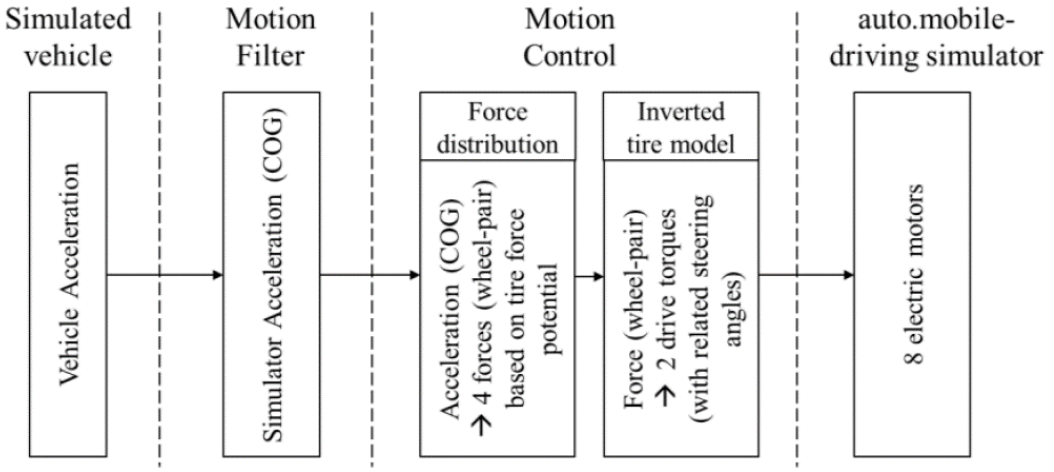

Figure 2-10: Control architecture of IAD's wheeled motion base DS[75c]

The suspension is designed as a passive two-stage double-wishbone suspension, Figure 2-11. Requirements to the suspension are identified to be isotropy (i.e. equal deflection behaviour in all directions), avoidance of pitch and roll movement (not to be noticed by

[75] Tüschen, T. et al.: Suspensions Design of a WMDS (2016). a: pp. 10f.; b: pp. 12f.; c: p. 12.

[76] Glatzki, F.: Bachelor's thesis, Trajektorienüberlagerung und Lenkleistungsbedarf eines WMDS (2016).

[77] Tüschen, T.; Prokop, G.: System Design of a Highly Dynamic DS (2014).

subject), good driving comfort (i.e. road excitation transmission to the subject below perception thresholds), and good driving dynamics (i.e. low variation in wheel load, explicitly no wheel lift-off). Especially the last two requirements are conflicting goals. This conflict is to be resolved by the two-stage suspension concept, whereas the lower double-wishbone suspension ensures good driving comfort and the upper double-wishbone suspension ensures good driving dynamics[78a].

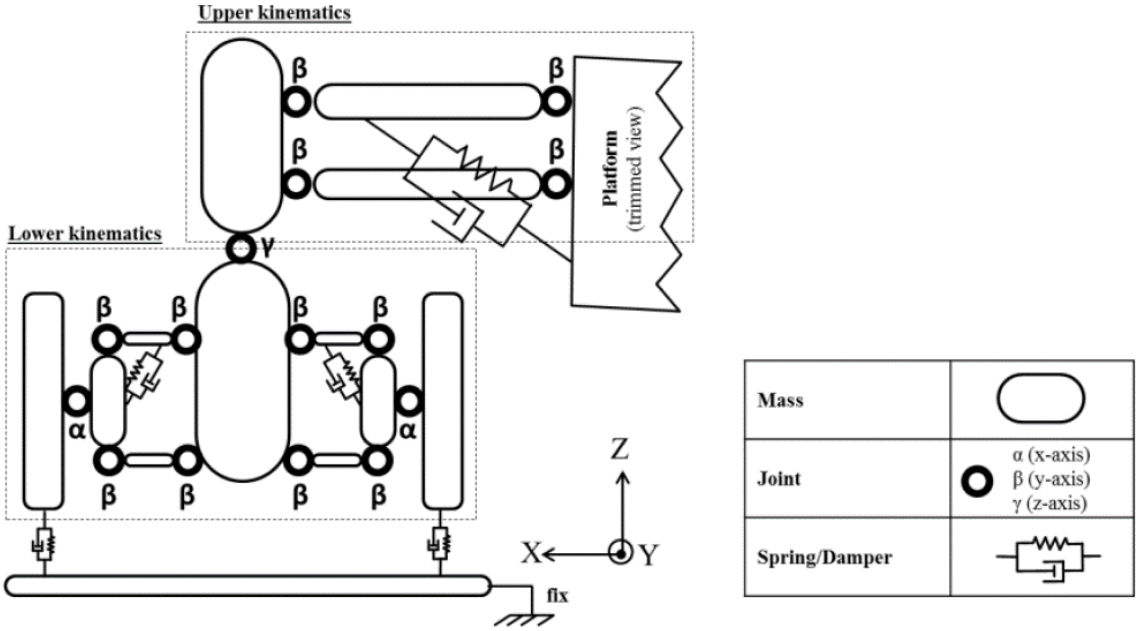

Figure 2-11: Dual suspension kinematics of IAD's wheeled motion base DS[78b]

The safety architecture of the unbound DS is addressed briefly in a patent that is held by AMST-Systemtechnik GmbH and Technische Universität Dresden together[79]. The main consideration is to bring the DS to an emergency stop, whereas the patent advises to build the trigger logic and trigger mechanism in a safe design. Three emergency braking methods are described:

1. Conventional wheel brakes: If the maximum friction coefficient is ought to be used and steering is not possible, wheel caster is required to provide course stability of the wheels. If the sliding friction coefficient is sufficient, on the one hand, the DS is not steerable in case of an emergency stop but on the other hand, a wheel caster does not influence the driving behaviour.
2. Brake plate: The wheels must not have contact to the driving surface. This can be done in two ways: By pressing the brake plate to the driving surface so that the simulator is lifted off the ground or by actively retracting the DS' wheels. The

[78] Tüschen, T. et al.: Suspensions Design of a WMDS (2016). a: pp. 15-18; b: p. 17.

[79] Tischer, W.; Prokop, G.: Selbstfahrender, hochdynamischer Fahrsimulator (2014). pp. 27f.

friction coefficient of the brake plate and the driving surface must be designed so that the DS cannot fall over in an emergency brake situation.

3. Braking bags: One or more inflatable braking bags are inflated in a short time, making contact to the driving surface and thus generating friction force. This method may be used alone or in combination with the first and second method.

2.2.8.5 Technische Universität Darmstadt, Department of Control Systems and Mechatronics

Technische Universität Darmstadt's department of control systems and mechatronics (Fachgebiet Regelungstechnik und Mechatronik, rtm) researches an alternative approach to WMDS based on omniwheels. Omniwheels (similar to Mecanum wheels) have cylinders located over their circumference, whose axis of rotation coincides with a wheel's corresponding tangent. Therefore, a drive torque can be supported in the wheel's tangential direction, a wheel load in radial direction, but no lateral force in axial direction. Thus, the non-holonomic characteristic of conventional wheels is overcome, yielding omnidirectionality. A scaled, prototypical platform has been designed and built at rtm to research control strategies, Figure 2-12:

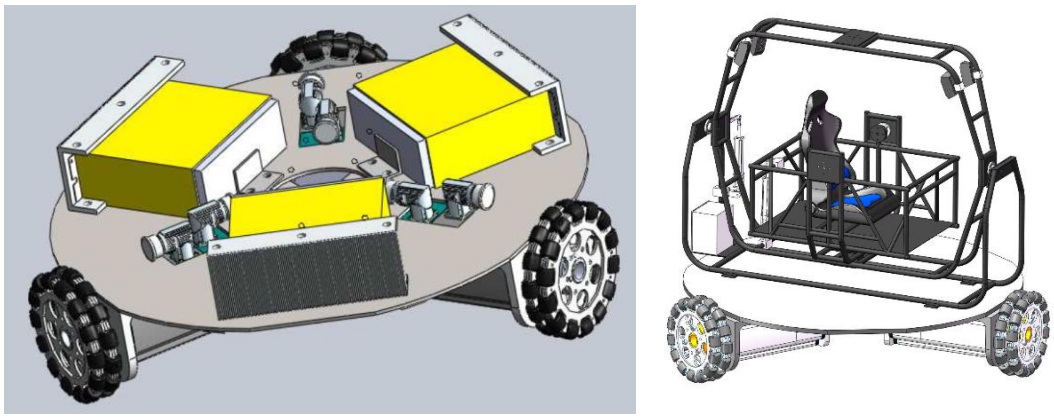

Figure 2-12: Left: CAD model of rtm's omnidirectional platform[80a]; Right: CAD model of rtm's wheeled motion base DS concept[81a]

Publications deal with the control structure with respect to high dynamic requirements, addressing tire characteristics, electrical components[80b], optimal control approaches[81b], as well as the replacement of the (classical) washout by two control loops[82] – one for TC and one for the platform – and comparing the novel approach to model predictive control MCA[83]. Figure 2-13 shows rtm's proposed control architecture:

[80] Gong, Z.; Konigorski, U.: Dynamic Modeling and Controller Design of WMDS (2016). a: p. 1533, b: - .

[81] Gong, Z.; Konigorski, U.: Modeling and Control of a WMDS (2017). a: p. 962; b: - .

[82] Gong, Z.; Konigorski, U.: Model-Based Control of a WMDS (2016).

[83] Gong, Z.; Konigorski, U.: Comparison of Different MCA in a WMDS (2017).

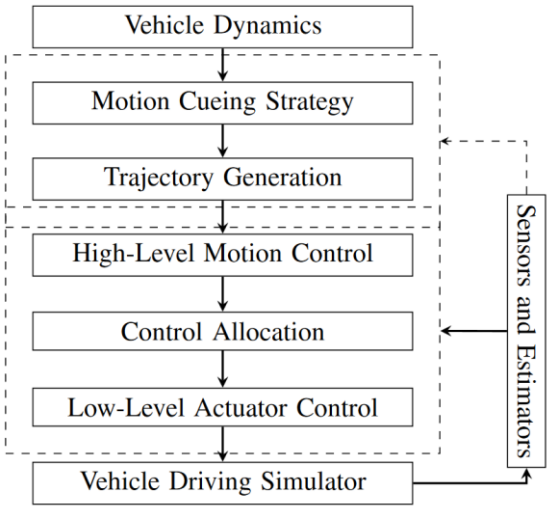

Figure 2-13: Hierarchical integrated control architecture of rtm's wheeled motion base DS[84]

The outcome of rtm's research proves that control architectures for unbound systems such as wheeled motion base DS exist and fulfil the dynamic requirements of driving simulation. Furthermore, they even bear the potential to gain an edge over state-of-the-art MCA approaches[85]. Unfortunately, the results are limited to omniwheels and cannot be directly transferred to non-holonomic wheels. Safety of wheeled motion base DS is not addressed by any of rtm's publications. Due to the principle of omniwheels, only 50 % of the available friction potential can be used, because not all wheels are oriented in driving direction. Thus, the force vector applied at the misaligned wheels contributes only partially to overcoming driving resistances. Given that with common rubber tires on common driving surfaces a friction coefficient of 1 is usually reached, an omniwheeled concept could only accelerate with 5 m/s², which is insufficient for unscaled, urban driving simulation. Furthermore, the discontinuous contact point at the wheels, which jumps from one cylinder to the next, is expected to cause vertical excitation, impeding the test person's immersion.

2.3 Functional Safety

Of course, design engineers want to construct safe systems. Two questions arise from this statement: Firstly, what does safe mean, and, secondly, how can a design engineer guarantee that the (possibly very complex) system is safe regarding the safety standard that must be defined to answer the first question. Many standards have been worked out for answering these questions and to give design engineers a guideline towards designing

[84] Gong, Z.; Konigorski, U.: Modeling and Control of a WMDS (2017). p. 962.

[85] Gong, Z.; Konigorski, U.: Comparison of Different MCA in a WMDS (2017).

safe systems. All safety standards have in common that the establishment of functional safety is partially rather intuitive and in general an iterative process. Graubohm et al. adopted their systematic design model for automated driving from the V-model presented in ISO 26262, Figure 2-14:

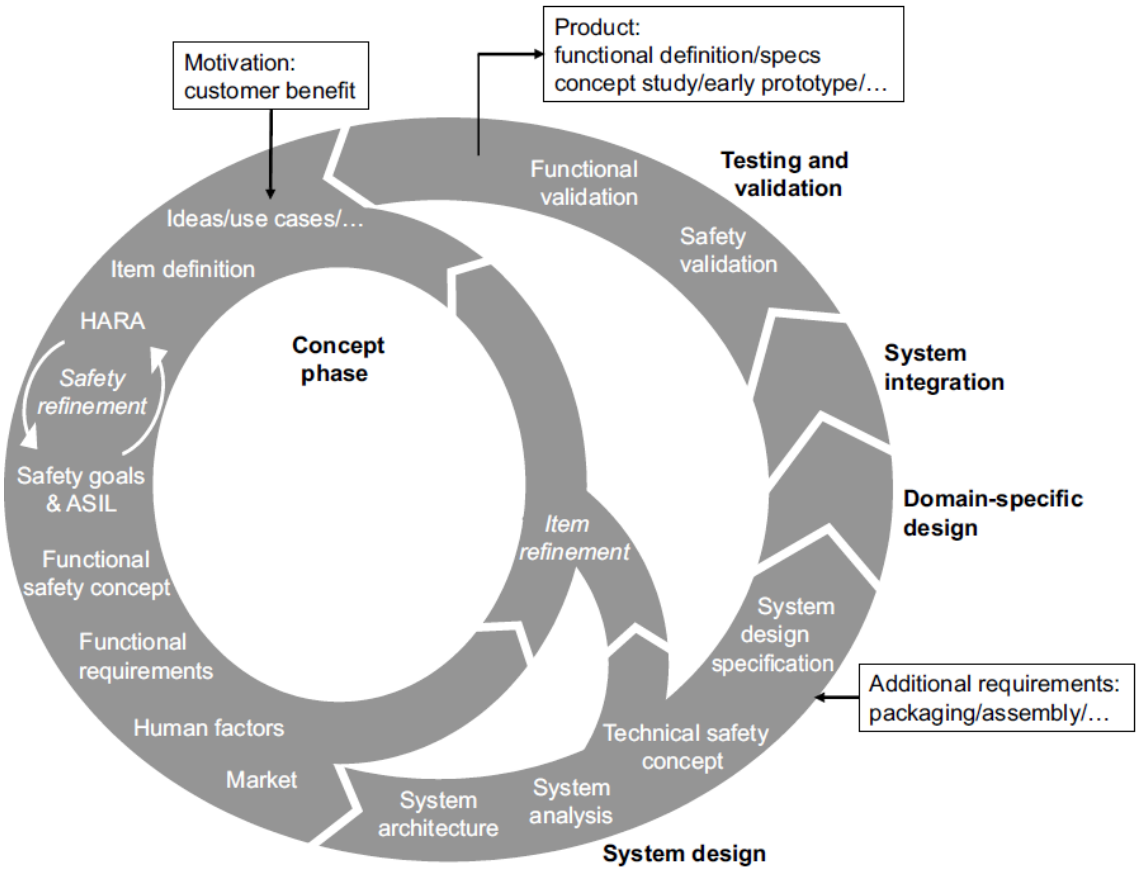

Figure 2-14: Systematic design model for automated driving functions[86]

Starting in the concept phase, use cases are established and the item is defined, followed by the Hazard And Risk Assessment (HARA). From here, safety goals are established, and a functional safety concept is developed that is broken down into functional requirements. Considering human factors and the market, a system architecture is developed, finally resulting in a technical safety concept. Instead of continuing the traditional path (system design and validation), Graubohm et al. added "shortcuts". Because detailed knowledge about the Equipment Under Control (EUC) is needed for the HARA, established safety goals are specific for the current version of the EUC, although the system design is preliminary. When the safety goals result in design changes, the HARA must be adapted, causing a tremendous effort if done after the validation phase. Therefore, these shortcuts help to accelerate the functional safety design process and make it more flexible.

[86] Graubohm, R. et al.: Systematic Design Considering Functional Safety Aspects (2017). p. 4.

Concluding, three axioms can be postulated for the design of functional safety:

1. Hazard identification is rather intuitive.
2. The design of functional safety is iterative.
3. A preliminary system design and understanding is needed for performing the HARA, although the goal of the process is to design a safe system based on the safety goals established from the HARA.

In the following, the most important functional safety standards with focus on the IEC 61508 will be described, preceded by the basic terminology that is needed for understanding the risk assessment process.

2.3.1 Terminology[87]

Consequence	The consequences and order of events triggered by an initiating failure
Controllability	Ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures
Element	A system or part of a system including components, hardware, software, hardware parts, and software units
Exposure	State of being in an operational situation that can be hazardous if coincident with the failure mode under analysis
Failure	Termination of an element to perform a function as required
Fault	Abnormal condition that can cause an element to fail
Functional safety	Absence of unreasonable risk due to hazards caused by malfunctioning behaviour of Electrical/Electronic/Programmable Electronic (E/E/PE) safety-related systems
Harm	Physical injury or damage to the health of persons
Hazard	Potential source of harm caused by malfunctioning behaviour of an element (combination of failure and its consequence)
Hazardous event	Combination of a hazard and a critical operational situation
Risk	Combination of the probability of a harm's occurrence and its severity
Safety function	A function, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event (cf. safety goal)

[87] Cf. ISO TC 22/SC 32 Electrical and electronic components and general system aspects: ISO 26262 (2011).

Safety integrity	The probability of a system satisfactorily performing the required safety functions
Safety goal	A top-level safety requirement resulting from the HARA (cf. safety function)
Severity	Estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation
Situation	A scenario that can occur during an EUC's lifecycle

2.3.2 IEC 61508

The international standard IEC 61508[88a], titled *Functional safety of E/E/PE safety-related systems*, has first been published in 1998. The standard enables engineers to investigate E/E/PE systems that perform safety functions and to evaluate the safety of such systems. It is suitable for all kinds of industry or products, so the standard may also be applied to hydraulic or pneumatic systems containing E/E/PE systems. Still, mechanical failure itself is not of interest in any functional safety standard because it is assumed that mechanical strength is assured by state-of-the-art design methods. The framework of the IEC 61508 adopts an overall safety lifecycle comprised of 16 phases (Figure 2-15):

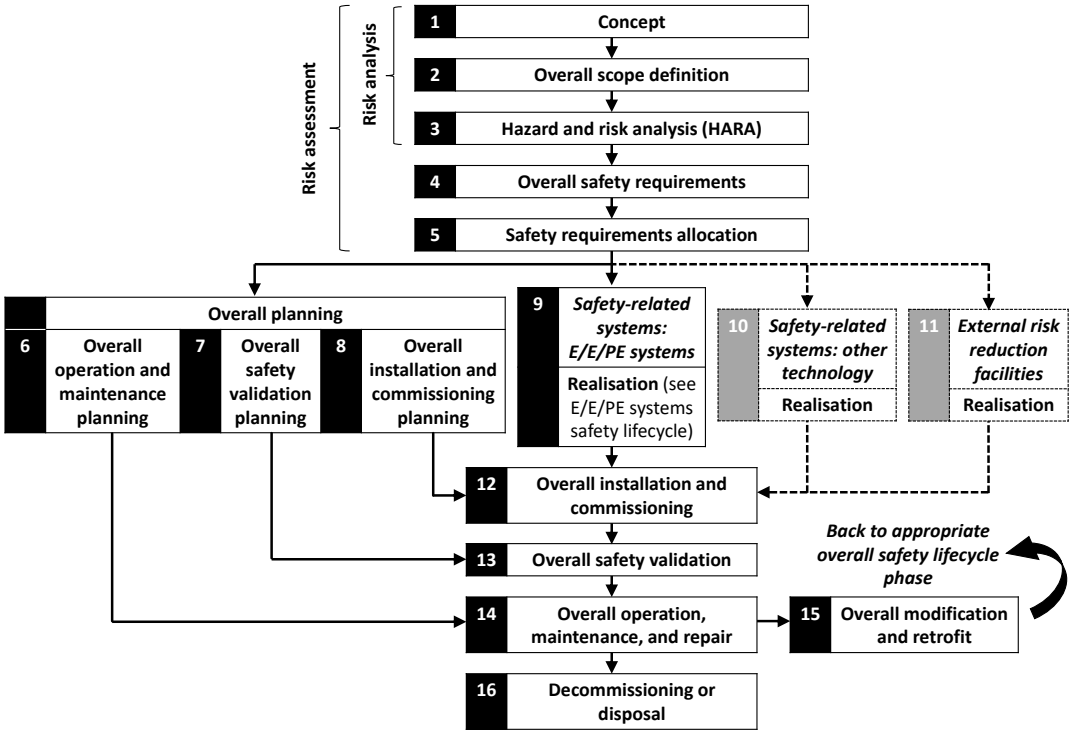

Figure 2-15: Overall safety lifecycle[88b]

[88] IEC TC 65/SC 65A - System aspects: IEC 61508 (2011). a: - ; b: p. 19.

The goal of the concept phase (Figure 2-15) is to acquire familiarity with the EUC by determining likely sources of hazards and obtaining information about those hazards. The overall scope definition determines the boundaries of the EUC and thereby sets the scope for the HARA. The objective of the HARA "is to determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse"[89a]. Furthermore, the event sequence leading to as well as the risks associated with the hazardous events are determined. Five informative risk assessment approaches are given: The ALARP-method, a general method, the risk graph method, a layer of protection analysis, and a hazardous event severity matrix, whereas the risk graph is the most commonly used, where the risk is qualitatively evaluated (Figure 2-16 with the risk parameters described in Table 2.4) and assigned to a Safety Integrity Level (SIL) (Table 2.5).

Table 2.4: Classification of risk parameters[89b]

Risk parameter		**Classification**
Consequence (C)	C1	Minor Injury
	C2	Serious permanent injury to one or more persons, death to one person
	C3	Death to several people
	C4	Very many people killed
Frequency of, and exposure time in the hazardous zone (F)	F1	Rare to more often exposure in the hazardous zone
	F2	Frequent to permanent exposure in the hazardous zone
Possibility of avoiding the hazardous event (P)	P1	Possible under certain conditions
	P2	Almost impossible
Probability of the unwanted occurrence (W)	W1	A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely
	W2	A slight probability that the unwanted occurrences will come to pass, and few unwanted occurrences are likely
	W3	A relatively high probability that the unwanted occurrences will come to pass, and frequent unwanted occurrences are likely

[89] IEC TC 65/SC 65A - System aspects: IEC 61508 (2011). a: p. 27; b: - .

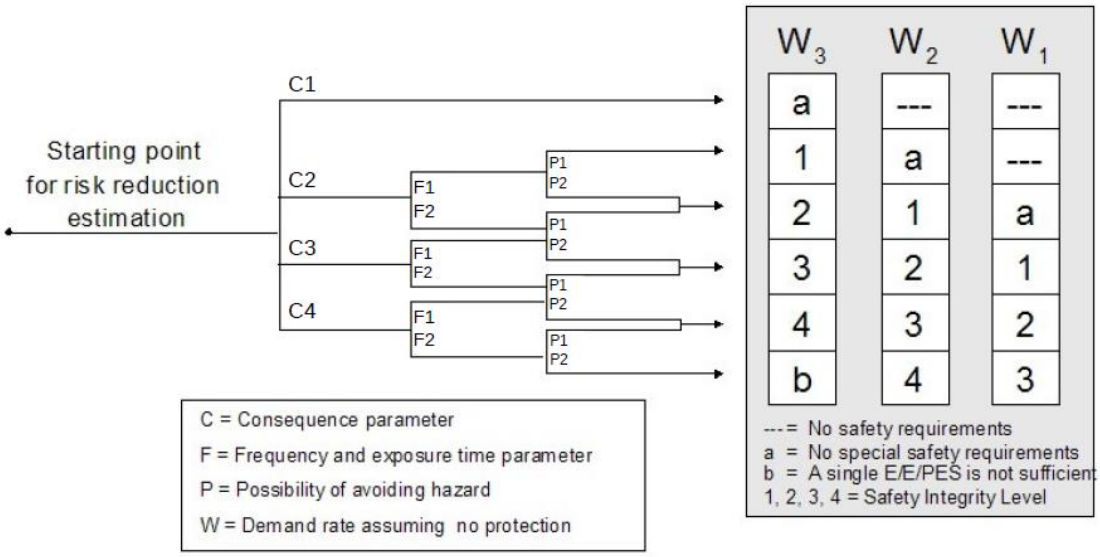

Figure 2-16: Risk graph general scheme[90]

Table 2.5: SIL: target failure measures for a safety function, allocated to an E/E/PE safety-related system[90]

	Probability of failure per hour	
SIL	Low demand mode of operation (≤1 demand per year)	High demand mode or continuous mode of operation (> 1 demand per year)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

The fourth phase “overall safety requirements” (Figure 2-15) develops the specification for the overall safety requirement, i.e. the safety requirements list, in which the safety functions for each hazardous event are described. The fifth phase allocates safety functions contained in the specification to designated E/E/PE or other technology safety-related systems and external risk reduction facilities while also allocating a SIL to each safety function. Phases six to eight deal with the planning of the operation, maintenance, safety validation, installation and commissioning of the E/E/PE safety-related system so that functional safety is maintained. The realisation phases (nine to eleven) create E/E/PE, other technology safety-related systems, and/or external risk reduction facilities conforming to the specification. The overall installation and commissioning phase is followed by the overall safety validation and the overall operation, maintenance, and repair phase. If the system is modified, phase 15 is triggered and the process must be restarted at the

[90] IEC TC 65/SC 65A - System aspects: IEC 61508 (2011).

appropriate overall safety lifecycle phase. The last phase deals with the decommissioning or disposal of the system.

2.3.3 ISO 26262

The international norm ISO 26262[91a], titled *Road vehicles – Functional safety,* is adapted from the IEC 61508 for the application to E/E/PE systems in the automotive industry where the ISO norm is widely used. The relationship to the IEC 61508 is noticeable throughout the standard, although some significant changes must be mentioned. For example, the risk graph is normative and therefore the only approach for risk evaluation in the ISO 26262. In addition, the risk parameters and their classifications are supplemented and amended. Finally, the Automotive Safety Integrity Level is introduced.

Still, the norm focuses on E/E/PE systems "that are installed in series production passenger cars [..] [and] does not address unique E/E systems in special purpose vehicles"[91b].

2.3.4 EN ISO 13849

EN ISO 13849[92] is a safety standard, titled *Safety of machinery -- Safety-related parts of control systems* (SRP/CS), and emerged from the DIN EN 954, which was first published in 1997. As the title already implies, the application of the standard is merely limited to control structures but may be applied to all technologies (not only E/E/PE). Still, the original purpose of the standard is intended for machinery. The EN ISO 13849 describes only one process for risk estimation, the risk graph, whereas the approach is informative. The overall method of risk reduction and the special method of risk graphs are well described within the standard. Figure 2-17 shows the risk reduction process that is preceded by the risk assessment, which can be divided into the risk analysis (determination of the limits of machinery, hazard identification, and risk estimation) and risk evaluation.

---

[91] ISO TC 22/SC 32 Electrical and electronic components and general system aspects: ISO 26262 (2011). a: - ; b: pt. 3, p. 1.

[92] ISO/TC 199 - Safety of machinery: EN ISO 13849 (2015).

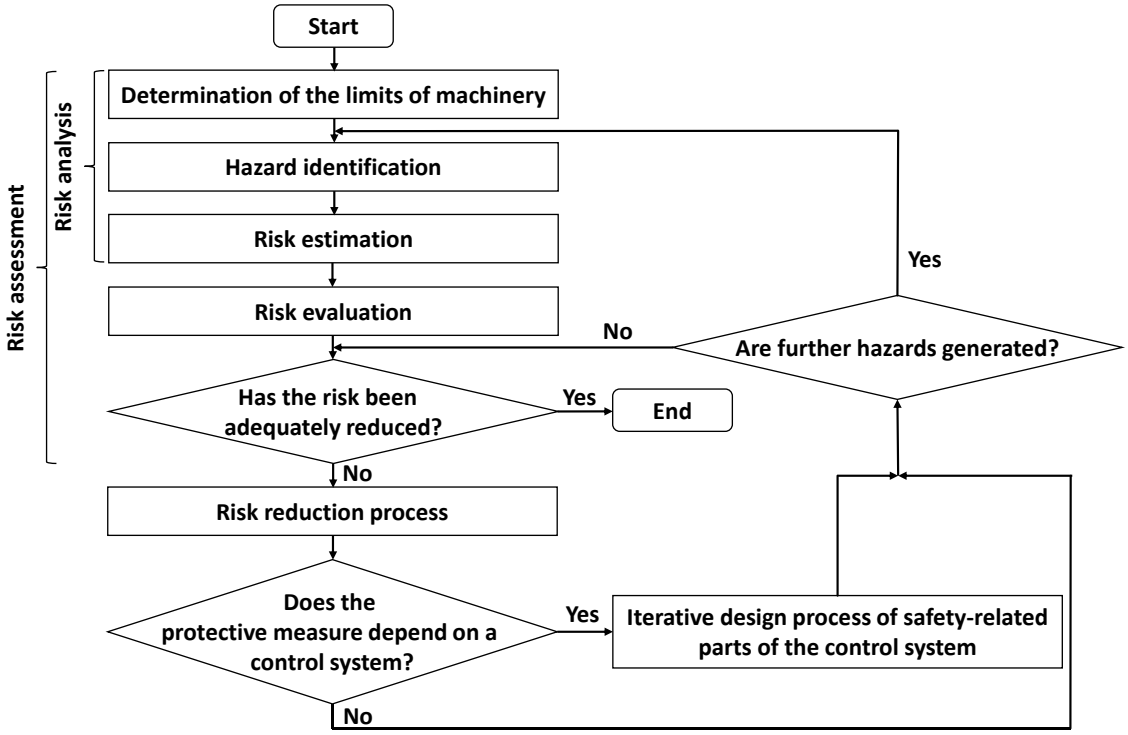

Figure 2-17: Risk reduction process per EN ISO 13849[93]

2.3.5 IEC/EN 62061

The IEC/EN 62061[94], titled *Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems,* is intended to help designing functional safety for any E/E/PE system. Risk assessment is not in the focus of the standard, which describes only one informative, qualitative method for risk evaluation (very similar to the risk graph method) resulting in a SIL according to IEC 61508, whereas the risk parameters are identical although with finer gradation.

2.3.6 IEC 61025

The IEC 61025[95], titled *Fault Tree Analysis (FTA),* describes a method to determine low-level events (e.g. failures) that lead to an undesired top-level event, ranking it as a deductive failure analysis. Boolean logic is used to link the events. The method is especially useful when analysing complex systems. Because the undesired top-level event must be

[93] Cf. ISO/TC 199 - Safety of machinery: EN ISO 13849 (2015).

[94] IEC TC 44 - Safety of machinery - electrotechnical aspects: IEC 62061 (2005).

[95] IEC TC 56 - Dependability: IEC 61025 (2006).

known prior to the analysis, the method is suitable to aid within any of the aforementioned functional safety assessment methods but cannot replace them.

2.3.7 IEC 60812

The IEC 60812[96], titled *Analysis techniques for system reliability – Procedure for Failure Mode and Effects Analysis (FMEA),* describes a failure analysis method based on a thorough review of components, subsystems, and processes, ranking it – in contrary to an FTA – as an inductive failure analysis. The method aims at identifying basic failures and evaluating their causes and effects on the system. The Failure Mode(s), Effects, and Criticality Analysis (FMECA) also evaluates the criticality of the failure and the subsequent events. Since the method has been developed in the 1950s', most of today's HARA methods are based on an FME(C)A.

2.4 Accumulator Technology

Due to current trends in the automotive industry, the development speed of battery cells has rapidly increased over the past years. Figure 2-18 shows the power and energy density of commonly used energy storage systems in a Ragone plot.

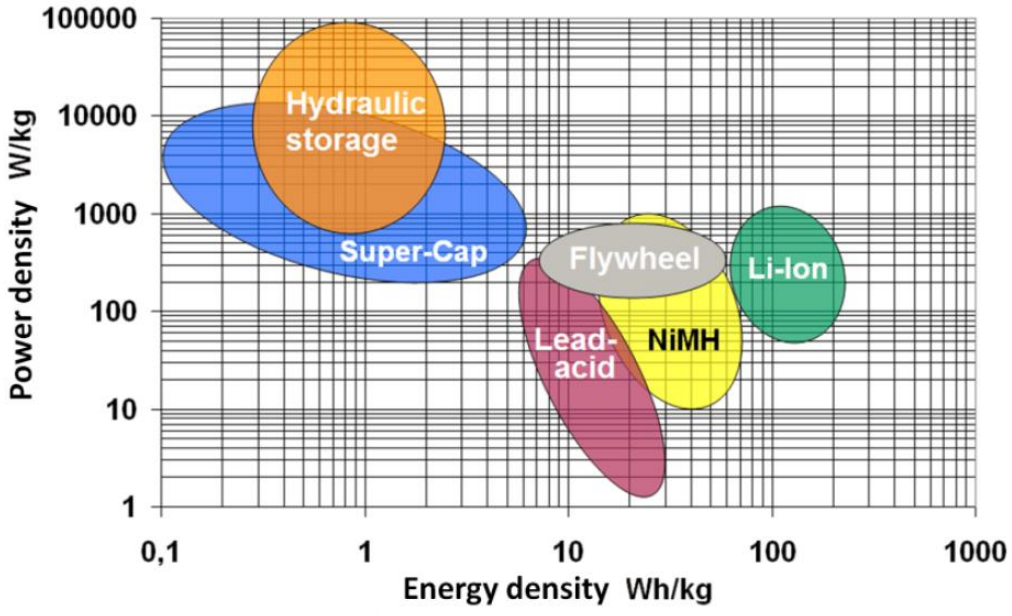

Figure 2-18: Ragone plot of commonly used energy storages[97]

[96] IEC TC 56 - Dependability: IEC 60812 (2006).

[97] Beidl, C.: Lecture Notes Combustion Engines II (2017). ch. 16, p. 13.

For mobile applications, like in a wheeled motion base DS, low mass is crucial. From Figure 2-18 can be seen that hydraulic energy storage systems as well as Super-Caps are in deficit when it comes to energy density. The remaining four energy storage types are similar in power density, whereas lithium-ion cells are superior when it comes to energy density. Current trends that are not mass-produced, yet, are lithium polymer, lithium iron phosphate, lithium titanite, lithium manganese, and nanostructure-based lithium cells[98a]. Advantageous are a higher energy and power density than with lithium-ion cells. The disadvantageous thermal and electrical sensitivity[98b] can be handled in a controlled environment of a DS, in which professionals are maintaining the DS instead of average car-owners. Finally, the cost for battery cells are expected to drop rapidly over the next decades, which makes the use of on-board accumulators even more feasible, cf. Figure 2-19.

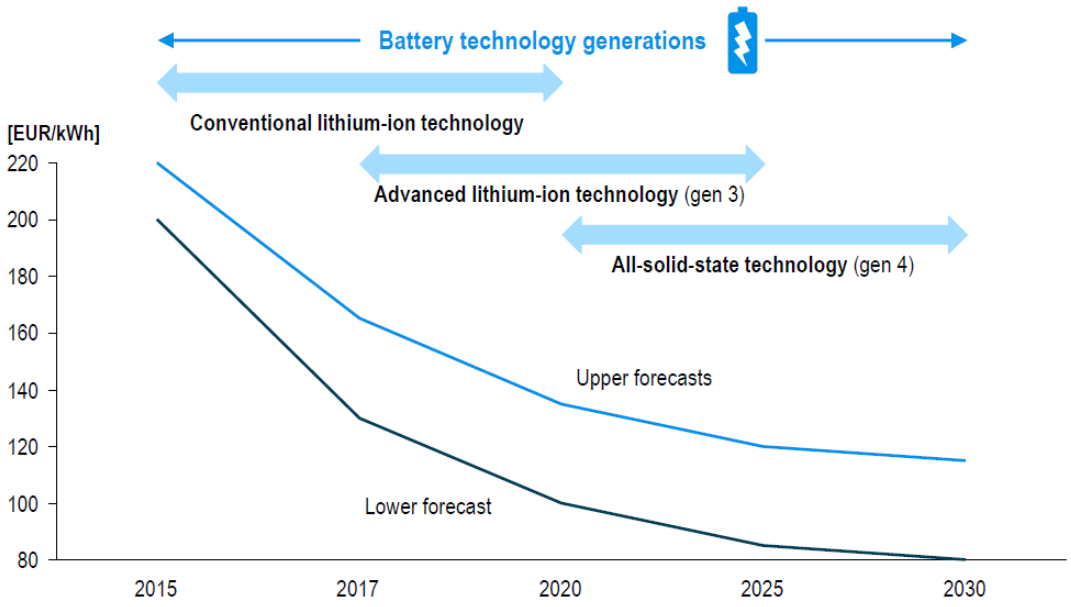

Figure 2-19: Cost forecast for battery cells per Roland Berger GmbH[99]

Another factor that must be considered is the desired duration of test drives and, therewith, the amount of energy that must be stored on the WMDS. “Typically researchers use the guidelines where drives should last between 5 and 25 minutes with 10 minute breaks”[100]. In any case, the total simulation exposure should not exceed 2 h to minimise the risk of simulator sickness[101]. Thus, the energy supplied by the main accumulator is desired to be sufficient for a maximum experiment duration of 2 h, until the accumulator must be recharged or substituted by a fully charged accumulator.

[98] Pfaffenbichler, P. C. et al.: Electric Mobility in Austria (2009). a: pp. 19f.; b: p. 19.

[99] van der Slot, A. et al.: Integrated Fuels and Vehicles Roadmap to 2030+ (2016). p. 37.

[100] Fisher, D. L.: Handbook of DS (2011). p. 14-17.

[101] Johnson, D. M.: Review of Simulator Sickness Research (2005).

2.5 Latency and Human Motion Perception

To reach a high immersion of the subject, all sensory organs must receive the same stimulus as they would in a real vehicle. Nevertheless, the goal of the ongoing research at FZD is to provide a novel simulator platform that can overcome limitations in motion rendering that are inherent to state-of-the-art DS, wherein this thesis is focused on the investigation of the motion performance and on the safety architecture. From this can be concluded that for understanding this thesis only motion perception is of relevance. As motion is only directly perceived by the vestibular organ, its function will be described followed by a summary of published perception thresholds and an evaluation of the role of latency in passenger cars.

2.5.1 Vestibular Organ

The vestibular organ is situated in the inner ear. It is composed of two larger swellings termed *utricle* and *saccule* as well as three semi-circular canals, each located in another orthogonal plane, whereas utricle and saccule sense translational and the semi-circular canals rotational accelerations, Figure 2-20.

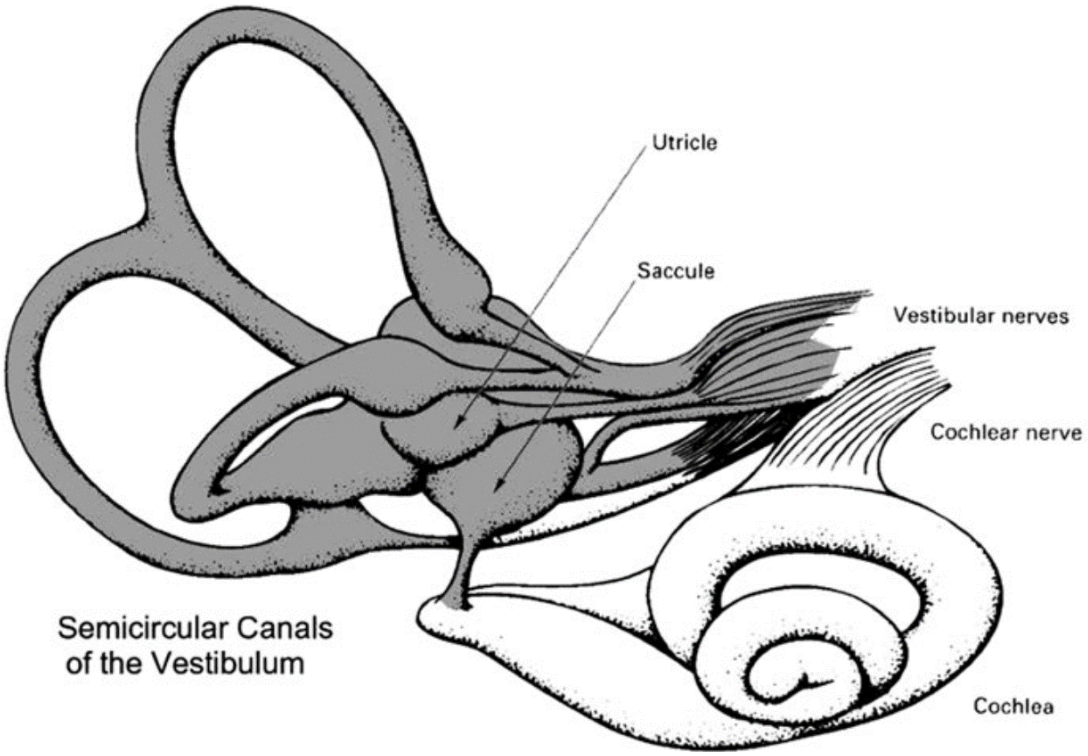

Figure 2-20: The vestibulum[102]

[102] Kroemer, K. H. et al.: Engineering Physiology (2010). p. 79.

Utricle and saccule are perpendicular and contain a region called *macula*. The macula is composed of a gelatinous layer, in which sensory hair cells are embedded, topped by a layer of calcium containing deposits called *statoconia* or *otoliths*. The macula of utricle is oriented horizontally, the macula of saccule vertically. The inertia of the statoconia causes the sensory hair cells to bend when the head is accelerated, thus sensing acceleration[103].

Rotational motion is sensed by the *cristae ampullares* that are located in each semi-circular canal, perpendicular to the canals' walls. The cristae ampullares are composed – similarly to the maculae – of a gelatinous mass, the *cupula*, in which sensory hair cells are embedded. When the head is rotating, the *endolymph* fluid in the semi-circular canals is flowing, causing the cristae ampullares and the embedded sensory hair cells to bend, thus, sensing rotational velocity[103].

2.5.2 Human Motion Perception Thresholds

The definition of static perception thresholds is a strenuous task, as already demonstrated by Fischer[104] and Betz[105]. This is due to manifold influencing factors[104], such as:

- Duration of exposure
- Subject's expectations
- Subject's physical condition
- Individual sensitivity
- Distraction
- Information from other sensory organs

For the sake of consistency and comparability, the same perception thresholds are used within this thesis as they were used by Betz[105], namely:

- Maximum tilt angle: $24° \triangleq 0.4\ g$
- Rotational velocity threshold: $6\ °/s$
- Rotational acceleration threshold: $6\ °/s^2$
- Translational acceleration threshold: $0.2\ m/s^2$

[103] Csillag, A.: Atlas of the Sensory Organs (2005). pp. 10f.

[104] Fischer, M.: Diss., MCA für eine realitätsnahe Bewegungssimulation (2009). p. 14.

[105] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). pp. 14ff.

2.5.3 Latency

Two thresholds are defined for latency in the motion system: An upper limit and a lower limit. Obviously, the upper limit is defined by the motion latency that can be felt in a real car, which is found to be 135 ms for longitudinal and 100 ms for lateral motion; a DS must stay below those values (section 2.5.3.2). However, there is also a lower limit because motion cues must not be provided prior to the corresponding visual cue, being 60 ms (section 2.5.3.1). While the upper limit is crucial to fulfil, the lower limit could also be reached by adding artificial latency in the control structure.

2.5.3.1 Visual Cues

Two types of visual representation systems are considered: Conventional display/video projector technology and head-mounted displays. For conventional display/video technology, latency refers to the time span from the user input via HMI to displaying visual changes resulting from the input. For HMDs, latency also refers to the time span from the user's head movement to displaying visual changes resulting from the head movement.

Literature reports that the detection of the driver's head movement may be reduced to less than 10 ms if optical sensors are combined with a gyro. Still, the traffic simulation needs about 50 ms for presenting the head movement in the virtual reality[106]. Another study showed that latencies above 267 ms are perceptible to most participants[107]. Thus, the latency in the motion system is desired to be within the range of 60 ms to 267 ms (lower motion latency bears no advantage since the calculation of the visual stimulus takes at least 60 ms and the motion cue must not be represented prior to the visual cue).

2.5.3.2 Acceleration Cues

The control inputs are given by the driver – in the real vehicle as well as in the DS. Thus, latency in the motion system is defined as the time span from the driver's acceleration demand (by brake pedal, acceleration pedal, steering wheel, etc.) to the actual presentation of the demanded acceleration. A DS' delay in acceleration representation is regarded to be sufficiently low if the values are below those of a real car and will be referred to as Acceleration Cue Latency (ACL). In any case (lateral or longitudinal motion), the time needed for calculating the control inputs in the MCA and MC must be accounted for. Also, if a physics-based vehicle model is used, inherent latencies, e.g. when using an elaborate tire model that takes relaxation lengths etc. into account, must not add to ACL. Thus, a latency model might be needed in the MC, resembling a feed forward control. Whereas the latter issue addresses the control and is therefore not dealt with in this thesis,

[106] Berg, G.; Färber, B.: Vehicle in the Loop (2015). pp. 160f.

[107] Wildzunas, R. M. et al.: Visual Display Delay Effects on Pilot Performance (1996). per St. Pierre, M. E. et al.: The Effects of Latency on Simulator Sickness in a HMD (2015). p. 1.

the latency added by calculating the control inputs must be included in the conducted investigation

2.5.3.2.1 Longitudinal Acceleration Cues

For longitudinal vehicle motion, deceleration and acceleration must be distinguished. Latency in deceleration is characterised by the sum of the brakes' response and build-up time (Figure 2-21), which depend on the brakes' actuation and force transmission system. The response time is the time span from brake pedal actuation to the first incline in vehicle deceleration. The build-up time is the time span from the first incline to full vehicle deceleration. Passenger cars usually need 200 ms for building up 50 % full vehicle deceleration ($t_{\mathrm{response}} + 0.5 \cdot t_{\mathrm{build-up}}$)[108], which defines the upper limit for longitudinal acceleration cue latency. This time span will be referred to as $t_{50\,\%}$ and the 50 % target acceleration criterion as the Indicator for 50 % ACL ($\mathrm{IACL}_{50\,\%}$, Figure 2-21).

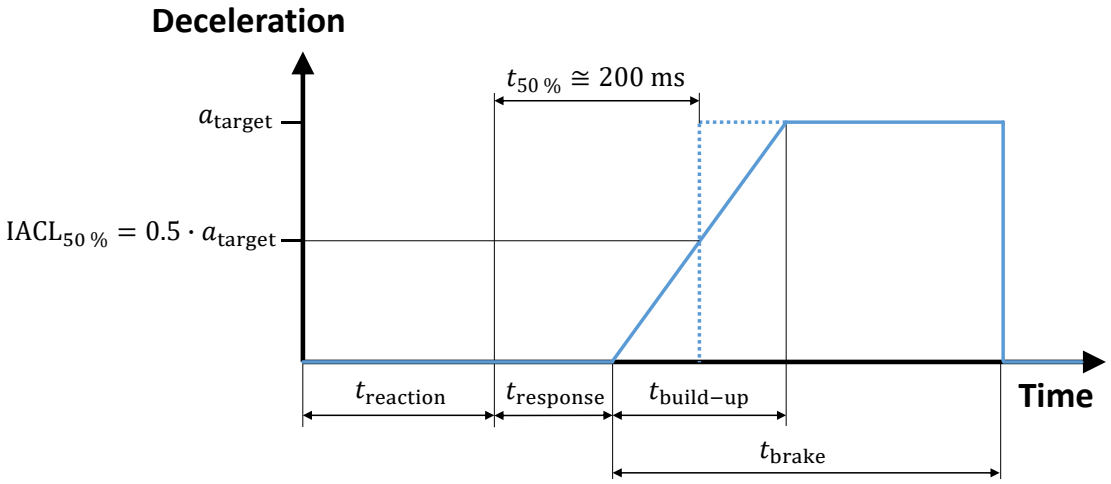

Figure 2-21: Deceleration during braking, cf. Breuer and Bill[108]

For acceleration, the case is more unclear since no standard values can be found in literature and a difference is expected for vehicles propelled by electric motors or internal combustion engines. Sato et al.[109] and Kawamura et al.[110] researched a highly responsive acceleration control for electric vehicles based on a unique shaking vibration control system. To prove the effectiveness of their control approach, they measured the acceleration response of an electric vehicle (Nissan LEAF) and a gasoline-propelled equivalent vehicle when fully accelerated from standstill, from constant driving at 20 km/h, and from

[108] Breuer, B.; Bill, K. H.: Bremsenhandbuch (2012). p. 17.

[109] Sato, Y. et al.: High Response Motor Nissan LEAF (2011).

[110] Kawamura, H. et al.: Highly-Responsive Acceleration Control for Nissan LEAF (2011).

coasting at 20 km/h. Hajek provides the same measurements for a full acceleration manoeuvre from constant driving at 20 km/h for a Tesla Model S[111a], a BMW ActiveE[111b], a BMW E92[111a], and a BMW E82[111b]. Applying the same criterion as for braking ($IACL_{50\,\%}$, time when 50 % of target acceleration is reached minus manoeuvre initiation time) yields the values in Table 2.6:

Table 2.6: Latencies for electric and internal combustion engine vehicles when accelerating, cf. Hajek[111a,111b], Sato et al.[112], and Kawamura et al.[113]

Initial driving condition	**Electric vehicle**		**Internal combustion engine vehicle**	
	$t_{50\,\%}$	**Vehicle**	$t_{50\,\%}$	**Vehicle**
Standstill	100 ms	Nissan LEAF	400 ms	Gasoline-propelled equivalent
$v = \text{const.} = 20\ \text{km/h}$	145 ms	Nissan LEAF	590 ms	Gasoline-propelled equivalent
	250 ms	Tesla Model S	500 ms	BMW E92
	280 ms	BMW ActiveE	360 ms	BMW E82
Coasting 20 km/h	135 ms	Nissan LEAF	525 ms	Gasoline-propelled equivalent

Unfortunately, the measurement run conducted by Sato et al. from standstill shows low longitudinal accelerations approximately 200 ms prior to manoeuvre initiation, impeding confidence in the results. Even more, latency from standstill is expected to be above latency from constant driving or coasting. Because the values found for acceleration with electric vehicles are below that of braking, 135 ms will be used as upper limit for ACL, when the $IACL_{50\,\%}$ is used for evaluation.

2.5.3.2.2 Lateral Acceleration Cues

For lateral vehicle motion, the time span from steering wheel input to the first yaw rate and/or lateral acceleration is used to evaluate the lateral response behaviour in passenger cars. Literature reports values between 82 ms and 138 ms for sports cars and 100 ms to 190 ms for regular passenger cars calculated from the frequency, at which the phase response between yaw rate and steering wheel angle is a phase angle of 45° in a frequency response test[114]. Thus, 100 ms is used as upper limit for lateral ACL because the primary purpose of a DS is not to simulate sports cars (normal driver behaviour, hypothesis H1.1, section 1.2.3.1). This time span will be referred to as t_{gain} and the criterion of an increase in the yaw rate and/or lateral acceleration as the Indicator for gaining ACL ($IACL_{\text{gain}}$).

[111] Hajek, H.: Diss., Längsdynamik von elektrifizierten Straßenfahrzeugen (2017). a: p. 70.; b: p. 73.

[112] Sato, Y. et al.: High Response Motor Nissan LEAF (2011). p. 8.

[113] Kawamura, H. et al.: Highly-Responsive Acceleration Control for Nissan LEAF (2011). p. 5.

[114] Pfeffer, P.; Harrer, M.: Lenkungshandbuch (2011). p. 140.

3 Wheeled Mobile Driving Simulator Prototype MORPHEUS

The basic concept behind a wheeled motion base DS has been explained in section 2.2.6. At FZD, a scaled prototype of a wheeled mobile driving simulator (WMDS) has been designed and manufactured for investigating the feasibility of the concept. The prototype is called MORPHEUS, which is the acronym for Mobile OmnidiRectional Platform for Highly dynamic and tirEboUnd driving Simulation. This chapter describes MORPHEUS and its architecture so that the reader is enabled to follow the outline of the falsification experiments for the wheeled motion base and the design of the safety architecture.

3.1 FZD's WMDS Concept

The concept idea has been developed by Betz et al.[115]. The core element of FZD's WMDS concept is an omnidirectional platform standing on three self-propelled and actively and infinitely steerable wheel units. Thus, the linkage between motion range and system mass is dissolved and, additionally, an infinite yaw DOF is created, improving urban driving simulation capabilities. The tilt system (for TC) in this concept can be reduced to three DOF, namely pitch, roll, and heave. A tripod is sufficient for providing these DOF.

3.2 MORPHEUS' Design

However, in the concept design for MORPHEUS decisions were made regarding requirements like sufficient system dynamics for urban driving simulation and safety, but also costs, ease of manufacturing, and/or availability of purchased parts. Thus, a hexapod was chosen over a tripod, because the range of available hexapods is larger than that of tripods and the additional DOF can be advantageous. E.g. missing or false cues from vertical excitation due to uneven road surface or from misaligned wheels can be masked[116]. A detailed description of MORPHEUS' development can be found in Wagner et al.[117].

[115] Betz, A. et al.: Concept Analysis of a WMDS (2012).

[116] Wagner, P. et al.: Potentials and Limitations of Hexapods in WMDS (2015).

[117] Wagner, P. et al.: Conception and Design of Mobile Driving Simulators (2014).

3.2.1 Wheel Units

For the platform design, the decision was made for three wheel units. On the one hand, costs are decreased because only three wheel units must be purchased and manufactured and on the other hand the calculation of wheel loads is unambiguous. Less wheel units would require active stabilisation of the system, whereas more wheel units would decrease the footprint of the platform. The resulting wheel unit design is shown in Figure 3-1, whereas the steering unit's Electric Motor (EM) and Gearbox (GB) are concentrically with the steering axis and the drive unit's EM and GB are axially aligned with the wheel's axis of rotation. This keeps the construction simple and reduces the moment of inertia around the steering EM's axis of rotation to a minimum.

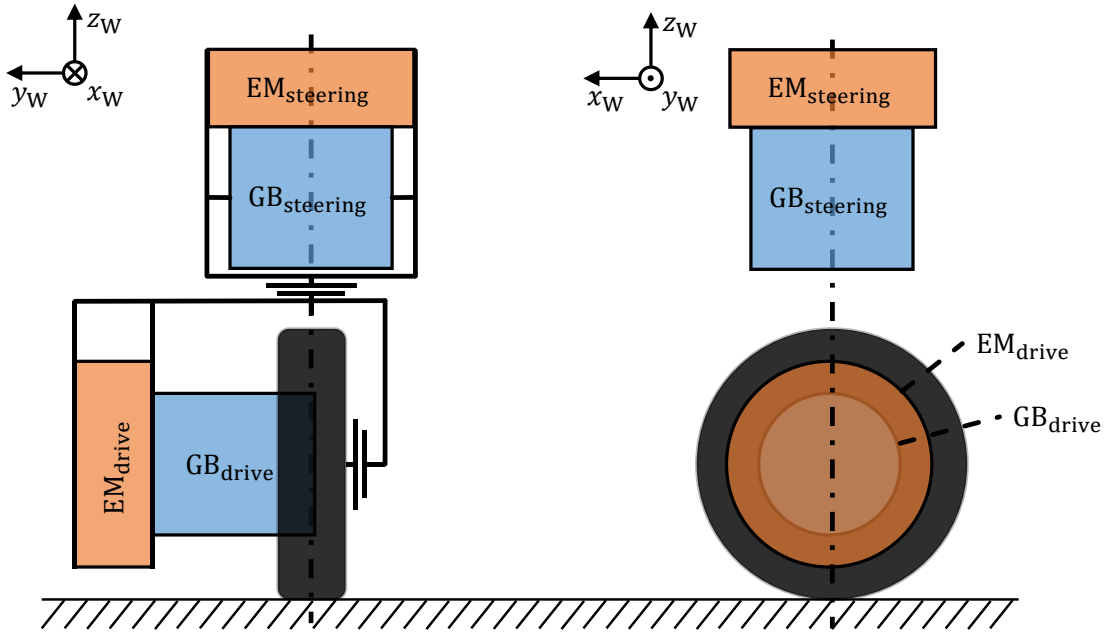

Figure 3-1: MORPHEUS' wheel unit design

Press-on band tires with their inherent high vertical stiffness are used instead of pneumatic tires with the aim of reducing unwanted pitch and roll movement. The wheel suspension is designed without spring and damper and no toe, camber, or caster is used to keep the design simple and cost efficient. Because of the omnidirectional approach – which implies an infinite steering angle – toe, camber, and caster are unwanted because they would cause anisotropy to the tire force transmission. Future designs may be equipped with sophisticated suspension designs to account for vertical excitations from uneven road surfaces.

3.2.2 Individual Components

Made-to-measure **slip rings** from RieTech are used for continuous power and information signal transfer to the electric drive motor and gearbox. INA XU 120179 **cross roller bearings** enable the steering DOF of the wheels. **All-steel couplings** of the type KTR Radex-

N 60 NNZ are installed at the gearbox torque output to account for production tolerances and negligent assembly. Furthermore, the load paths are unambiguous when couplings are introduced. The **hexapod** is purchased from Mevea and is of the type 6DOF 1200E with "no backlash" actuators. The **mock-up** is purchased from Fanatec and includes a frame on which a racing seat with a four-point safety belt is mounted. A BOSE sound system and three ASUS VE276N DVI monitors represent acoustical and visual cues. Driver inputs are measured by a ClubSport steering wheel with shift paddles and force feedback, and ClubSport CSP V2 pedals (clutch pedal with potentiometer, brake pedal with ABS actuator and load cell (adjustable in resistance), accelerator pedal with potentiometer (adjustable in resistance)). Table 3.1 gives an overview of MORPHEUS' drive train components from energy storage to force transmission to the driving surface:

Table 3.1: MORPHEUS' drive train components

Component		**Value**	**Unit**
Accumulator (reproduction of TU Darmstadt Racing Team e.V. (DART) lithium polymer accumulator)	Number of cells	144	./.
	Nominal output voltage	532.8	V (DC)
	Nominal output current	140	A
	Maximum output voltage	600	V (DC)
	Maximum output current (20 s)	200	A
	Capacity	10	Ah
Electric motor controller (UniTek BAMOCAR D-3-700-250)	Rated supply voltage	700	V (DC)
	Rated output voltage	400	V (AC)
	Continuous current	125	A
	Peak current	250	A
Electric motor (Enstroj EMRAX 228 high voltage air-cooled with LTN RE-15-1-A15 resolvers)	Peak power	100	kW
	Continuous power	55	kW
	Peak torque	240	Nm
	Continuous torque	125	Nm
Gearbox (Neugart PLFN-140-5 with minimum backlash option)	Transmission ratio	5	./.
	Max. torque all-time	1,200	Nm
	Max. torque short-time	1,500	Nm
Tire (Gumasol Softy 300/75-15 with made-to-measure rims by Pneuhage)	Radius	0.15	m
	Width	0.075	m
	Vertical stiffness	1,036	N/mm

3.2.3 Hardware System Architecture

Figure 3-2 and Figure 3-3 show the power transfer respectively data transmission architecture for the MORPHEUS prototype.

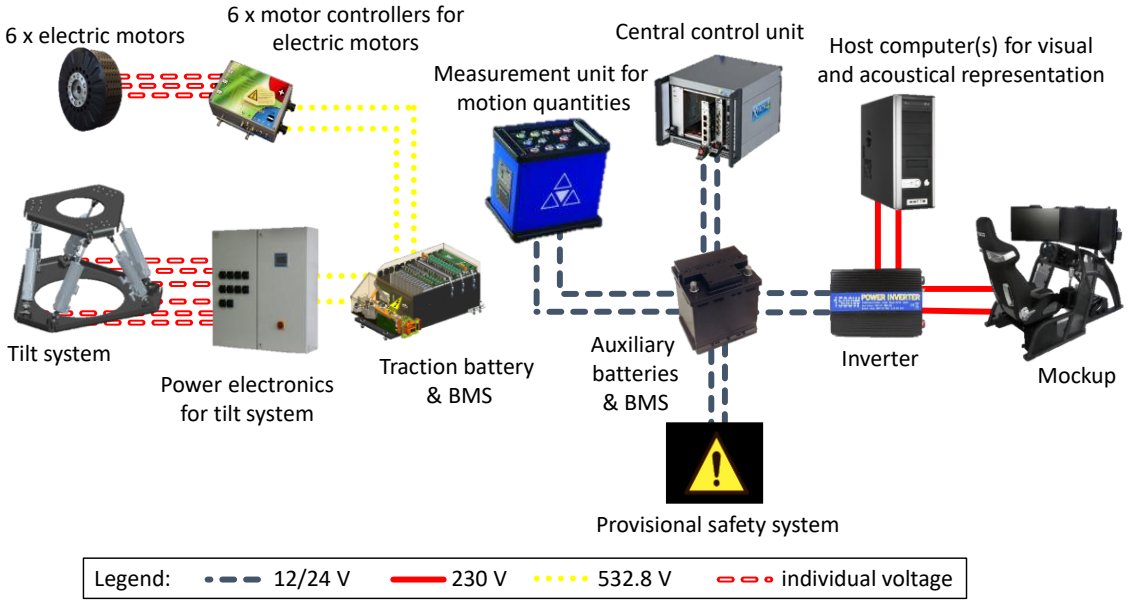

Figure 3-2: MORPHEUS' power transfer architecture[118]

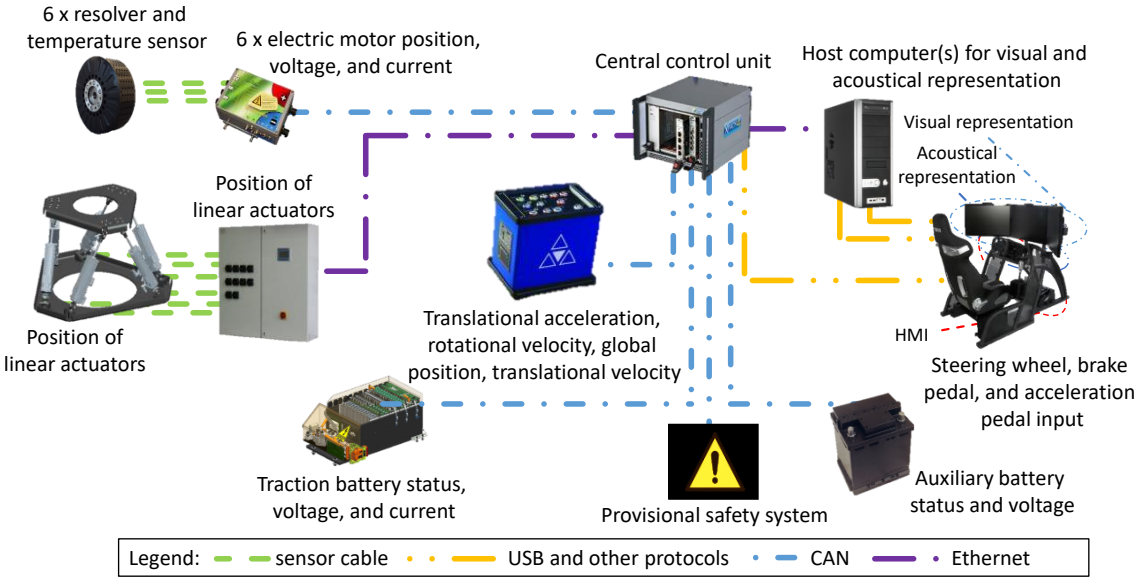

Figure 3-3: MORPHEUS' data transmission architecture[118]

[118] cf. Wagner, P.: Master's thesis, Aufbau und Inbetriebnahme eines WMDS (2013).

3.2.4 Summary

Figure 3-4 shows a photograph of the MORPHEUS prototype with installed provisional safety system, and hexapod, but without mock-up, as of April 2015.

Figure 3-4: MORPHEUS prototype[119]

The maximum height of the platform triangle (including all attachment parts) is just below 2.4 m, which makes the prototype transportable via truck. The height of the Center Of Gravity (COG) is 0.481 m and the total mass of MORPHEUS is 1,302 kg, whereas the mass distribution is given in the next section in Table 3.3. This setup assures overturning stability for horizontal accelerations of about 13.5 m/s², whereas the tire-road friction coefficient is limited to values of about 0.8[120,121] (see annexe A). The verification manoeuvres (section 6) are driven without hexapod power electronics, mock-up, and subject, resulting in a reduced system mass of 1,056 kg. Driving performance figures are given in Table 3.3, too.

3.3 Motion Cueing Algorithm

3.3.1 Structure

„The applied MCA is similar to the classical washout. The so-called ‘ideal’ MCA[122] (Figure 3-5) calculates the target DS states that are necessary to perform the target motion

[119] Wagner, P. et al.: Potentials and Limitations of Hexapods in WMDS (2015). p. 132.

[120] Betz, A. et al.: Konzeptanalyse und Erprobung eines WMDS (2014).

[121] Zöller, C. et al.: Tire Concept Investigation for WMDS (2016).

[122] Betz, A. et al.: Motion Analysis of a WMDS (2012).

cue input. The goal is a frequency-independent acceleration simulation […]. By closing the frequency gap of the MCA, the created driving experience is no longer subject to the occurring frequencies. In general, this 'ideal' MCA provides a more realistic acceleration simulation at the cost of increased workspace demand. The characteristic of the new MCA suits the system-immanent motion capability of the WMDS"[123a].

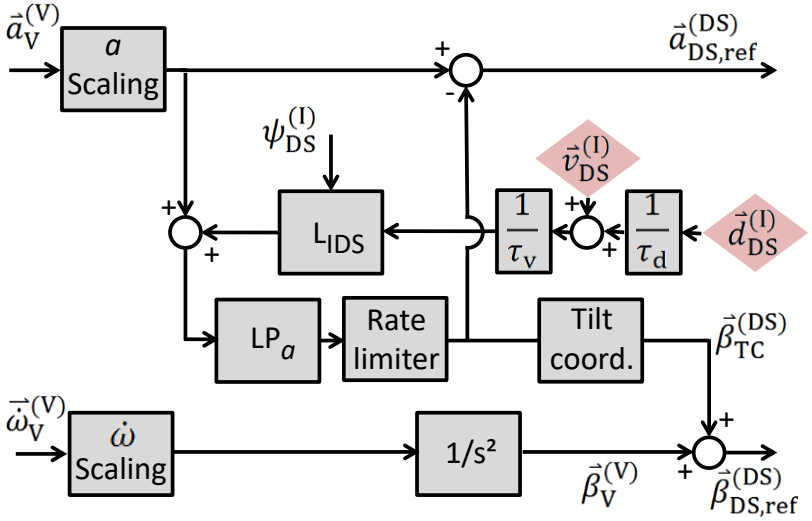

Figure 3-5: "ideal" MCA[123b]

3.3.2 Parameterisation

The MCA's feedback gains are tuned for urban driving scenarios (see section 5.1.2). For details, see Betz[123c].

- $\tau_v = 4.49$ s
- $\tau_d = 19.77$ s

The Low-Pass (LP) filter LP_a of the form (3-1) is tuned depending on the chosen scaling factor and urban driving scenarios, whereas $n = 120$ refers to 120 threshold violations per hour simulation, see Table 3.2.

$$G_{LP}(s) = \frac{1}{1 + 2dTs + T^2s^2} \tag{3-1}$$

[123] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). a: pp. 51f.; b: p. 51; c: pp. 52-58.

Table 3.2: Parameterisation of low-pass filter in dependence on urban driving scenarios and scaling factor[124a]

Urban test drive #	Scaling	$d_{n=120}$	$T_{n=120}$ in $\frac{1}{s}$
1	1.0	1.49	1.60
	0.7	1.16	1.33
	0.5	0.93	1.14
2	1.0	1.49	1.60
	0.7	1.18	1.34
	0.5	0.94	1.15
3	1.0	1.38	1.49
	0.7	1.10	1.26
	0.5	0.88	1.09
4	1.0	1.34	1.44
	0.7	1.07	1.22
	0.5	0.86	1.05

3.4 Motion Control

The MC translates the motion signals generated by the MCA into control inputs for the actuators, namely drive torque $M_{\mathrm{W,drive},i}$ and steering angle $\delta_{\mathrm{W,dyn},i}$. Because the MC is not to be investigated within this work, only a short summary of the constraints and process is given. For a detailed description, see Betz[124b] and Betz et al.[125,126].

Constraints:

- Equal exploitation of the wheels' friction capability
- Linear tire characteristics

Process:

(0. Transformation of acceleration and yaw demand of the virtual car (as demanded by test person) to acceleration, yaw, and tilt demand of WMDS in the MCA.)

[124] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). a: p. 58; b: pp. 58-70.

[125] Betz, A. et al.: Concept Analysis of a WMDS (2012).

[126] Betz, A. et al.: Driving Dynamics Control of a WMDS (2013).

1. Transformation of acceleration and yaw demand from MCA into a horizontal force acting on and a yaw torque acting about the WMDS' COG.
2. Transformation of the yaw torque to horizontal tire forces under the constraint of equal exploitation of the tires' friction capability (under consideration of dynamic wheel loads) and calculation of the overall required tire force.
3. Calculation of kinematic steering angles (neglecting dynamic effects, e.g. slip) from the WMDS' yaw rate and velocity vector.
4. Estimation of longitudinal tire force demand and slip angles based on the overall required tire force and the kinematic steering angles through a numerical optimisation (linear lateral tire model).
5. Calculation of drive motor torques from longitudinal tire force demand and the dynamic tire radius.
6. Calculation of steering motor angles from kinematic steering angle and slip angle.

3.5 Control Architecture

A closed-loop acceleration controller has been developed by Betz et al.[127] but could not guarantee stability in the MORPHEUS prototype. Since no closed-loop control is needed for the scope of this thesis, an open-loop acceleration control is used instead. The motor controllers are tuned according to the values provided by the electric motors' manufacturer, controlling the electric motors' speed.

3.6 Scaling to Full-Size WMDS

As mentioned earlier, the MORPHEUS prototype is scaled down in size and power from the full-scale WMDS concept with the intention of keeping costs low while still being able to investigate feasibility. Besides the scaled size, the major difference is the lack of a proper cabin on MORPHEUS. Because a head-mounted display is ought to be used, no vehicle cab is used on MORPHEUS and the HMI can be reduced to a minimum. However, for the full-scale WMDS, a closed dome and a simplified vehicle mock-up will be used to enable the usage of virtual reality methods. In an initial investigation, no pneumatic tires could be found that can fulfil the requirements to wheel load, maximum velocity, and desired tire radius. Thus, a twin wheel solution is evaluated. The geometry, electric motors, and accumulator are re-evaluated and amended to fulfil the requirements for over-

[127] Betz, A. et al.: Driving Dynamics Control of a WMDS (2013).

turning stability, experiment duration, acceleration, and velocity. Table 3.3 shows the parameters that resulted for this full-scale WMDS concept compared to those of MORPHEUS:

Table 3.3: Properties of scaled MORPHEUS prototype compared to the full-scale WMDS concept

Property	MORPHEUS prototype with reduced visual representation system for validation reasons (motion base research)[128,129]	Full DS with enhanced visual representation system for DS studies (DS application: studies with subjects)[130]
Overall mass	1,302 kg	2,604 kg
Cabin[131]	173 kg	393 kg
Hexapod	145 kg	350 kg
Frame	576 kg	347 kg
Wheel units (incl. suspension)		600 kg
Power supply & electronics	208 kg	674 kg
Emergency braking system	200 kg	240 kg
Height of COG	0.48 m	0.796 m
l_t	2.3 m	4.8 m
Overall height	1.95 m	3.42 m
Wheel radius	0.15 m	0.281 m
Maximum accumulator power	104.5 kW	300 kW
Accumulator capacity	5.3 kWh	40 kWh
Traction motor power	300 kW (Peak-Sum)	690 kW (Peak-sum)
Steering motor power	300 kW (Peak-Sum)	690 kW (Peak-sum)
90° steer step delay	< 0.1 s	< 0.1 s
Max. acceleration	~8 m/s²	~8 m/s²
Max. velocity	~12 m/s	~20 m/s

[128] Cf. Wagner, P.: Master's thesis, Aufbau und Inbetriebnahme eines WMDS (2013).

[129] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 79.

[130] Cf. Hein, E. et al.: Advanced Design Project, Entwicklung des unskalierten WMDS (2017).

[131] Including test person, mock-up, air conditioning (only for full-scale WMDS), visual and acoustical representation system

4 Methodology

This chapter describes the experimental setup and evaluation criteria for the falsification experiments of the wheeled motion base (sections 4.2 and 4.3, adopted from Wagner et al.[132]). Section 4.4 describes the risk assessment process as it is applied in chapter 7.

4.1 Power Demand

The drive power must be sufficient to provide the maximum acceleration and maximum velocity required to represent urban driving scenarios with common scaling factors. Betz identified the maximum acceleration and velocity required for representing urban driving scenarios with different scaling factors in simulation[133a]. Only the MCA and MC (cf. sections 3.3 and 3.4) were used for determining the velocity and acceleration demand, therefore, the results are not influenced by the fact that Betz conducted the simulations for the unscaled WMDS. The results of all four urban driving scenarios are merged and can be interpolated with a linear regression when acceleration or velocity are plotted in a log-log diagram against the scaling factor, Figure 4-1 and Figure 4-2 (resulting in a power function of the scaling factor with an exponent of the slope value):

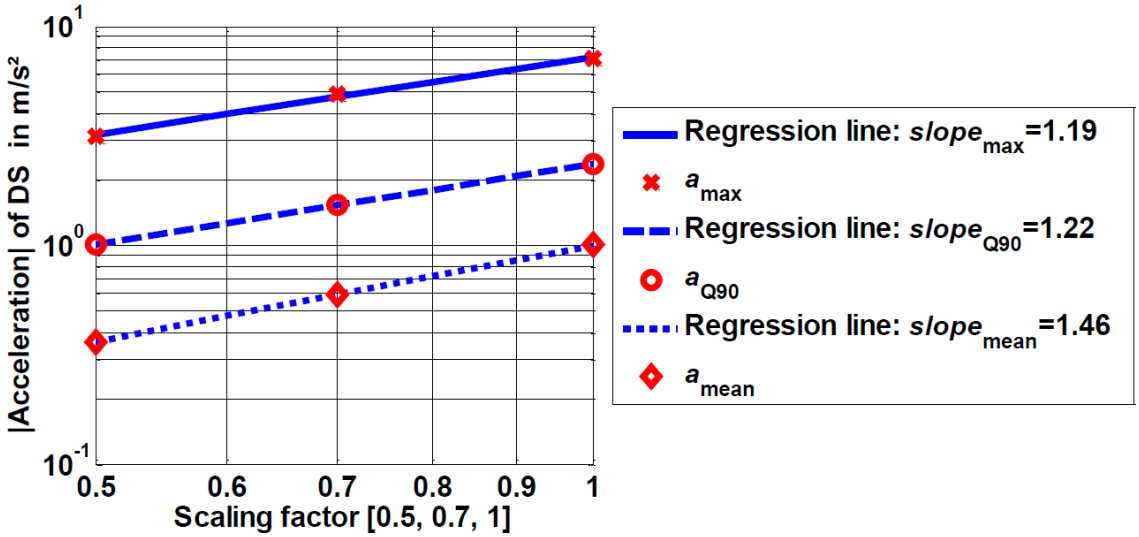

Figure 4-1: Power function regressions for acceleration and scaling factor in urban driving scenarios[133b]

[132] Wagner, P. et al.: Power, Energy, and Latency Test Drives with MORPHEUS (2017).

[133] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). a: pp. 105-115, b: p. 109.

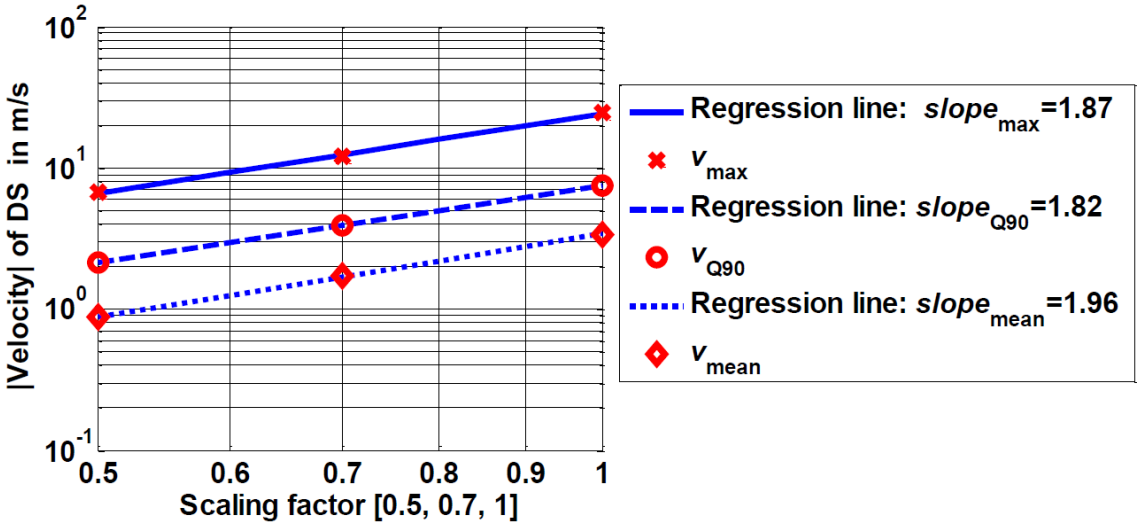

Figure 4-2: Power function regressions for velocity and scaling factor in urban driving scenarios[134]

For unscaled urban driving scenarios, a maximum velocity of 24.7 m/s and a maximum acceleration of 7.1 m/s², for a scaling factor of 0.7 a velocity of 12 m/s and an acceleration of 4.9 m/s², and for 50 % scaling 6.8 m/s and 3.1 m/s² are sufficient. This shows that the velocity demand of unscaled urban driving scenarios cannot be fulfilled by MORPHEUS, because its maximum velocity is limited to about 12 m/s (Table 3.3). Furthermore, the HV accumulator's output power limits the overall propulsion power (3 x 100 kW electric motor power), as can be seen when calculated: The minimum operating voltage is used because measurements show that the accumulator's output voltage drops to this value when the maximum current is drawn from the accumulator. Interestingly, the experiments revealed that the maximum current drawn from the accumulator peaked at 242 A and coincided with the voltage drop. The accumulator's maximum power is then calculated to:

$$P_{\text{accumulator}} = U_{\min} \cdot I_{\max} = 432\ \text{V} \cdot 242\ \text{A} = 104.5\ \text{kW} \qquad (4\text{-}1)$$

Therefore, a Matlab Simulink based power/energy model is integrated into the virtual prototype and improvements are made to the IPG CarMaker model (section 5.2.4) for identifying the power demand (section 6.2). The model takes several effects into account that can be grouped into four categories:

1. Electric power demand of electric motors and motor controllers
2. Driving speed dependent power demand from driving resistances
3. Mechanical power demand from steering and self-aligning torque

[134] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 109.

4. Mechanical power demand at wheel hubs, accounting for slip losses and translational as well as rotational acceleration resistance

These effects are parameterised by conducting synthetic manoeuvres (namely coasting experiments, holding torque experiments, and straight-line acceleration experiments, section 6.1.1) with MORPHEUS and measuring the platform's energy demand. Simple straight-line driving manoeuvres (section 5.1.1.1) with constant acceleration are conducted to verify the power model (section 6.1.2.1).

The aspect *power demand* falsifies hypothesis H1.1 if FZD's WMDS concept cannot represent the required maximum acceleration and velocity amplitudes with state-of-the-art technology.

4.2 Energy Demand

Energy is converted by the platform, the hexapod, and auxiliaries. Because the available driving area is not sufficient to drive unscaled urban driving scenarios (section 5.1.2) with MORPHEUS – which constitute the most realistic application with maximum energy demand – the virtual prototype is used to determine the platform's energy demand by integrating the power model over time. The resulting energy model is validated by conducting scaled synthetic and representative manoeuvres (namely a 90° turn, a figure eight, and an urban driving scenario, sections 5.1.1.4, 5.1.1.5, and 5.1.2) with MORPHEUS and comparing the measured energy demand to the simulated energy demand (section 6.1.2.2). Finally, the maximum energy demand of MORPHEUS is determined by simulating unscaled, representative urban driving scenarios with the validated energy model (section 6.3.1). The overall energy demand is then calculated by adding the estimated demand of the hexapod and the measured energy demand of Low Voltage (LV) auxiliaries (e.g. safety system, power electronics, measurement technology) (section 6.3.2).

The aspect *energy demand* falsifies hypothesis H1.1 if the results from the verified energy model prove that unscaled urban driving simulation cannot be represented with state-of-the-art accumulator technology for at least 2 h, considering state-of-the-art technology.

4.3 Acceleration Cue Latency

To identify the worst-case latency in the motion system, synthetic manoeuvres are used with MORPHEUS. Because of the omnidirectionality of WMDS, the latency requirements cannot be clearly divided into longitudinal and lateral motion. Even more, latency is expected to depend on the wheels' orientation and to behave identical for lateral and

longitudinal motion cues. In contrast, a passenger car has a distinctive orientation, hence latency is different for lateral and longitudinal motion, and different measurement indicators are used for determining lateral and longitudinal motion latency. Therefore, the manoeuvre with the worst-case latency must be identified for MORPHEUS, analysed with the gaining and 50 % criteria for ACL, and evaluated for the minimum acceleration latency as it can be found in passenger cars (section 2.5.3.2). Section 4.3.1 describes the difference in latency between WMDS and passenger cars in detail and therewith identifies the manoeuvre with the worst-case latency for MOPRHEUS. Sections 4.3.2 to 4.3.4 describe the experimental setup, the evaluation methodology and give a conclusion, respectively.

4.3.1 Latency in a WMDS and in a Passenger Car

Latency in a WMDS' acceleration representation arises from delayed force transmission in the desired direction. This delay is influenced by the response behaviour of the electric motors and by the wheel units' current state of operation. The response behaviour can be influenced by the control parameters that are tuned iteratively. The wheel units' state of operation is strongly dependent on the current DS state and can be discriminated into seven cases in dependence on the yaw angle, acceleration demand, and WMDS velocity:

1. Identical yaw angle in DS' COS as in vehicle's COS:
   1.1. Lateral acceleration demand
      1.1.1. WMDS driving velocity well above zero: Like in a real car, slip angle must be generated at the wheels to build up lateral tire force.
      1.1.2. WMDS driving velocity close to zero: Whereas the vehicle's driving velocity is high enough for building up sufficient lateral tire force through slip angle, the WMDS' wheels must re-orientate so that they align with the desired direction of motion to provide the lateral acceleration using the drive motor. For re-orientating the wheels, the steering unit's friction torque, the tire's drill torque and the moment of inertia must be overcome.
   1.2. Longitudinal acceleration demand: The drive motors must only overcome the drive unit's friction torque and moment of inertia. The remaining drive torque can be used for acceleration. The driving velocity has no influence on latency, given that the motor power is sufficient for accelerating.
2. Different yaw angle in DS' COS as in vehicle's COS (can only occur with a low-frequent acceleration demand → washout is active):
   2.1. Lateral acceleration demand

2.1.1. WMDS driving velocity well above zero: Lateral tire force can be generated by slip angle, although the wheels must be re-orientated first by less than 90°. The steering unit's friction torque, the drill torque, and the moment of inertia must be overcome.

2.1.2. WMDS driving velocity close to zero: In the worst case, the wheels are perpendicular to the desired direction of motion and must be re-orientated first. The steering unit's friction torque, the drill torque, and the moment of inertia must be overcome.

2.2. Longitudinal acceleration demand: 2.2.1 and 2.2.2 as with lateral acceleration demand (case 2.1.1 and 2.1.2).

Clearly, cases 1.1.1 and 1.2 are least critical. For cases 1.1.2 and 2 the latency that is also caused in case 1.2 (drive unit's friction torque and moment of inertia) is supplemented by the latency needed for re-orientating the wheels – in a worst-case by 90° (steering unit's friction torque, drill torque, and moment of inertia must be overcome). Figure 4-3 demonstrates the difference in tire force transmission for a lateral acceleration step input in a real vehicle (or virtual vehicle, left) and a WMDS (right), which is equivalent to case 1.1.2. When lateral acceleration is demanded in a moving vehicle, the wheels are steered into the desired direction, thus generating slip angle leading to the build-up of lateral tire force and, therewith, lateral acceleration. In the WMDS, however, the local yaw angle does not necessarily comply with the vehicle's yaw angle. Still, the overall vestibular driving impression, in this case especially the horizontal acceleration, must correlate. Due to the washout, the WMDS' velocity can be reduced to near zero if the WMDS' accelerations match the vehicle's acceleration (superposed by TC) plus or minus the human perception threshold for translational acceleration $a_{\mathrm{threshold}}$.

Concluding, the worst-case latency occurs when the wheels are misaligned by 90° to the desired direction of acceleration and the driving velocity is near zero. As demonstrated in Figure 4-3 the side slip angle of WMDS can reach 90°, unlike a regular passenger car. Therefore, it is sufficient to measure the worst-case latency for either longitudinal or lateral acceleration, which is why only lateral acceleration step inputs are used in the experiments. Nevertheless, different acceptable latency limits apply for lateral and longitudinal acceleration in a real car. Thus, the lateral acceleration experiments are analysed with the criteria for gaining (t_{gain}, $\mathrm{IACL}_{\mathrm{gain}}$) and 50 % ($t_{50\,\%}$, $\mathrm{IACL}_{50\,\%}$) acceleration cue latency and evaluated with the minimum lateral and longitudinal acceleration latency of a real car.

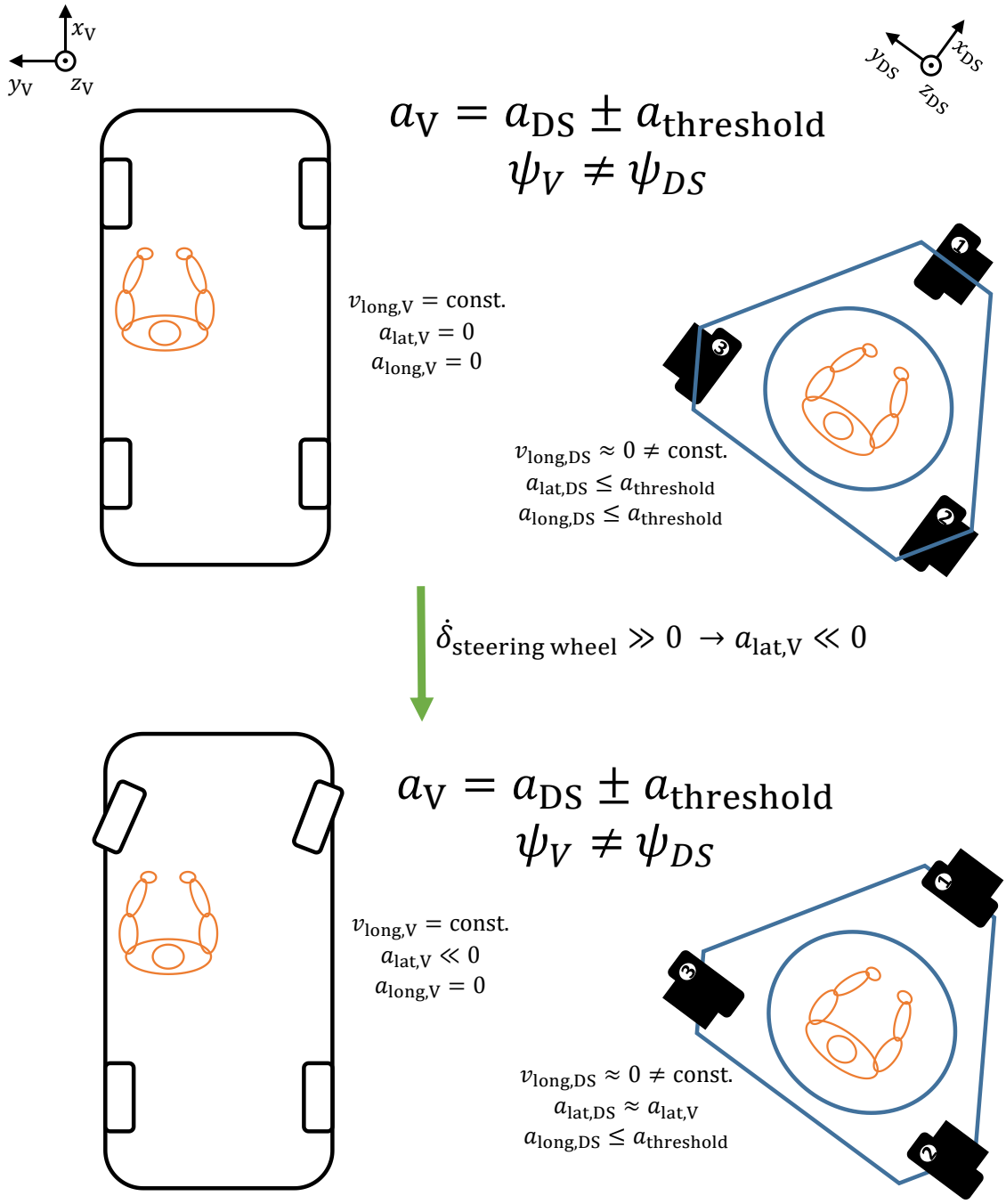

Figure 4-3: Lateral acceleration step input in a vehicle (left) and a WMDS (right) for the initial state (top) and the required state for providing the desired acceleration (bottom)

4.3.2 Experiment Design

The influence of two variables is of interest: Firstly, the amplitude of the acceleration step input, and secondly, the initial driving velocity at manoeuvre initiation. Furthermore, the type of the target signal might have an influence, namely an acceleration step input and a

steering angle step input. Therefore, an experiments design is chosen so that a minimum number of experiments clarifies how latency is influenced in a WMDS:

1. Variation of lateral acceleration step input amplitude from 1 m/s² to 8 m/s² in 1 m/s² increments and with an initial longitudinal velocity of 0 and 1 m/s.
2. Variation of initial longitudinal velocity
    a. with an acceleration step input amplitude of 5 m/s² and with initial longitudinal velocities of 0 to 6 m/s in 1 m/s increments.
    b. With a 90° (i.e. maximum) steering angle step input with initial longitudinal velocities of 1 m/s to 6 m/s in 1 m/s increments.

Thus, the first experiment investigates the influence of the acceleration step input amplitude in detail and the influence of the initial longitudinal velocity at low speeds. Higher speeds are not driven because the most significant influence of the initial velocity is expected at low speeds due to the drilling torque. The second experiments investigate the detailed influence of longitudinal velocity up to medium speeds for one acceleration step input and steering angle step input and thereby also investigates the influence of the type of control input. Thus, it can be proven if the assumption of negligible influence of the initial velocity at speeds above 1 m/s is valid.

4.3.3 Experiment Assessment

$ACL_{50\,\%}$ is calculated by subtracting the manoeuvre initiation time (e.g. acceleration step input) from the time when 50 % of the target acceleration is reached ($IACL_{50\,\%}$). For calculating ACL_{gain}, an indicator to determine the time when the system is reacting to the control input is needed, too. Latency is then calculated as the difference between the time of indication and the time of manoeuvre initiation. In passenger cars, the first increase in yaw rate or lateral acceleration is used as an indicator for the vehicle's reaction to the control input. Because lateral motion in a driving simulator is not necessarily connected to yaw motion, it is advisable to use lateral acceleration as an indicator instead. This assumption is eligible because in a car yaw motion is induced by lateral acceleration making the investigation conservative. Since the overall aim is to represent acceleration to a human test person, it is obvious to use the human perception threshold of 0.2 m/s² (cf. section 2.5.2) as an indicator, yielding $IACL_{gain}$.

All experiments are analysed with the $IACL_{50\,\%}$ and the $IACL_{gain}$. For experiment 2a (variation of the initial longitudinal velocity with a steering angle step input), however, a target steering angle is set instead of a target acceleration. Therefore, $IACL_{50\,\%}$ is defined as the time when 50 % of the maximum acceleration resulting from the steering angle step input is reached, yielding a conservative value.

4.3.4 Summary

Each experiment is carried out six times, yielding 174 data sets for evaluating $ACL_{50\,\%}$ and ACL_{gain}.

The aspect *motion cue latency* falsifies hypothesis H1.1 if the hardware prototype cannot reach 50 % of any acceleration step input within 135 ms and 0.2 m/s² after any acceleration or steering angle step input within 100 ms at any velocity, considering state-of-the-art technology.

4.4 Risk Assessment

The most relevant safety standards have been introduced in section 2.3. The ISO 26262 is intended for automotive series production and is therefore not ideal for prototypes. The EN ISO 13849 and the IEC/EN 62061 are focussed on E/E/PE control systems. Thus, the IEC 61508, which is often referred to as the "mother standard for E/E/PE system safety", is applied.

Risk assessment is dealt with in IEC 60300 "Dependability management", whereas the part most important for HARA, the IEC 60300-3-9 "Risk analysis of technological systems", has been evolved into the ISO/IEC 31010 "Risk management – Risk assessment techniques"[135]. The ISO/IEC 31010 proposes a total of 31 risk assessment techniques that can also be found in Ericson's "Hazard analysis techniques for system safety", which is more focused on the overarching safety aspects rather than functional safety. Ericson states "one of the annoying truisms of system safety is that it is usually easier to mitigate a hazard than it is to recognize or find the hazard in the first place"[136]. Therefore, the goal is to identify hazards to the fullest extent possible. Although structured approaches, e.g. Figure 2-17, exist, 100 % safety cannot be guaranteed. This makes it even more important to be thorough on elaborating each and every step in the risk assessment process.

The focus of this thesis is on functional safety and, therefore, the chosen methodology is closer to IEC 61508 than to the elaborate methods as described by Ericson. The risk graph is the only risk estimation method that is described in all aforementioned standards and will be used here as well. The structure, as chosen with sections 4.4.1 to 4.4.4, is adapted from EN ISO 13849 (cf. Figure 2-17). A sufficient mechanical strength of the components

[135] ISO/TC 262 - Risk management: IEC 31010 (2009).

[136] Ericson, C. A.: Hazard Analysis Techniques for System Safety (2005). p. 24.

is assumed. Faults like loose connectors and/or worn through cables are not included directly. Still, signal dropouts are a matter of functional safety and, therewith, take faulty cables/connectors indirectly into account.

4.4.1 Determination of the Limits of Machinery

The determination of the limits of machinery can also be found in the overall safety lifecycle in IEC 61508 (Figure 2-15), represented by phases one and two: concept and overall scope definition.

Ericson describes a hazard triangle[137] that is comprised of three elements:

1. Hazardous element: A basic hazardous resource, e.g. energy
2. Initiating mechanism: The trigger or initiator event(s)
3. Target and threat: The person or thing that is vulnerable to injury and/or damage

Only if all three elements are present, a hazard can arise. Knowing about these basic elements enables the design engineer to search the system for them. Generic checklists can help because possible hazards that can be caused by single elements are pointed out. This also underlines the importance of determining the limits of the system under investigation properly, including:

- System components (structural elements)
- System design (flow of forces, energy, information)
- System functions (what is the system intended/designed to do?)
- Energy sources (electric, hydraulic, pneumatic, chemical, etc.)
- Concepts for operation (who will be using the system with which expertise and in which mode, e.g. regular operation, maintenance, repair, transport, etc.)
- External conditions (e.g. climate, electromagnetic compatibility, etc.)

The results of this process are a complete description of the EUC, likely sources of hazards (hazardous elements, initiating mechanisms, and targets and threats), and information about the current safety regulations.

4.4.2 Hazard Identification

A hazard is defined by a failure (e.g. no power supply) and the consequence of the failure (in this case no acceleration/deceleration or steering possible). The hazard identification is included in the third phase, HARA, of the overall safety lifecycle in IEC 61508 (Figure 2-15). Clause 7.4.2.1 of IEC 61508 states if “decisions are taken [...] which may change

[137] Ericson, C. A.: Hazard Analysis Techniques for System Safety (2005). p. 17.

the basis on which the earlier decisions were taken, then a further HARA shall be undertaken"[138], underlining that conducting a HARA is an iterative process. Ericson advises to utilise past knowledge, evaluate top-level mishaps and finally yet importantly use generic hazard (source) checklists, also provided by Ericson. Still, the process of risk analysis, especially hazard identification, is rather intuitive; the predominant method for hazard identification is brainstorming, although supported by structured approaches leading through the identification process, e.g.:

- Dividing complex systems into subsystems and precisely working out the information and power flow between and within the subsystems.
- Splitting components into sensors, actuators, and electronic control units.
- Evaluating possible failures that could arise from the component's intended functions.
- Conducting FTA or FME(C)A

Conducting the hazard identification in a team of experts increases the probability of identifying all relevant hazards. The IEC 61822 "Hazard and operability studies (HAZOP studies) - Application guide"[139] gives a guideline towards structured and systematic examination of hazards. For identifying hazards, twelve guidewords are introduced. If a guideword is applicable to an intended function of the EUC, the combination of the two must be reviewed to find out if it constitutes a hazard to the system. The guidewords are:

Table 4.1: Guidewords for hazard identification[139]

Guideword	**Meaning**
NO OR NOT	Complete negation of the design intent
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative modification/increase
PART OF	Qualitative modification/decrease
REVERSE	Logical opposite of the design intent
OTHER THAN / INSTEAD	Complete substitution
EARLY	Relative to the clock time
LATE	Relative to the clock time
BEFORE	Relating to order or sequence
AFTER	Relating to order or sequence

[138] IEC TC 65/SC 65A - System aspects: IEC 61508 (2011). p. 27.

[139] IEC TC 56 - Dependability: IEC 61882 (2016).

As an example, the function *supply demanded power to drive motor* is investigated. For this function, it must be investigated if it constitutes a hazard in case no/more/less power is supplied, power as well as or as part of another signal is supplied, power is drawn rather than supplied, another signal instead of power is supplied, or power is supplied late/early or before/after a specific event.

The result of the hazard identification is a – to the best of one's knowledge – complete list of all hazards, whereas the situation, in which each hazard occurs, is not of interest, yet.

4.4.3 Risk Estimation

The risk estimation is also included in the third phase, HARA, of the overall safety lifecycle in IEC 61508 (Figure 2-15). The goal of the risk estimation is to assign each hazard that has been identified in the previous process (section 4.4.2) to a risk level. The combination of a hazard and a critical operational situation yields a hazardous event, whose risk can be evaluated. It is not advisable to list each possible situation, because most situations will be uncritical and are not worth looking at. Therefore, the expert conducting the analysis may choose the most critical situation. If it is unclear which situation is the most critical, it is also valid to extend the hazard to a few situations.

The definition of the risk level depends on the standard (performance level in EN ISO 13849, automotive SIL in ISO 26262, or SIL in IEC 61508), whereas the SIL will be used in this thesis. In any case, a hazard's consequences, its probability of occurrence (the situation and the mishap), and its controllability must be evaluated. If no valid data exists for evaluating these hazard parameters (which usually is the case), a qualitative evaluation is performed by estimating the level of each risk parameter. As with the hazard identification, this process is rather intuitive and decisions about allocations can be argued. The most common qualitative method for evaluating the risk level (independent of the chosen metric) is the risk graph, Figure 2-16. In addition, a solution for mitigating each risk is formulated.

The result of the risk estimation is a – to the best of one's knowledge – complete list of all hazards that includes – for each and every hazard – a description of the situation, an evaluation of the risk/assignment of a risk level, and a proposal of a risk reduction method.

4.4.4 Risk Evaluation

The risk evaluation includes the fourth and fifth phases, namely overall safety requirements and safety requirement allocation, of the overall safety lifecycle in IEC 61508 (Figure 2-15). The goals are to establish the overall safety requirements (or safety goals according to ISO 26262) and to evaluate if the overall risk that arises from the system has

been adequately reduced. The overall safety requirements are comprised of the safety functions requirements (i.e. the function that is intended to reduce the risk, derived from the hazard analysis) and the safety integrity requirements (i.e. the risk reduction required (SIL in case of IEC 61508), derived from the risk analysis). At this stage, the safety function must not be specified in technology-specific terms. Also, the definition of the safety functions must be done regardless of the hazardous event's situation. Otherwise, the safety function could reduce the risk of the specific hazardous event, but not the risk of other hazardous events that are associated with the same failure and consequence but in different, less critical situations (which possibly result in a lower SIL and are therefore not listed in the HARA). If the risk has been adequately reduced, no further measures are needed. If not, a risk reduction process is triggered (Figure 2-17). The architectural or processual changes that are made within the risk reduction process may require an additional risk assessment process or a re-assessment of the whole EUC.

The result of the risk evaluation is a – to the best of one's knowledge – complete overall safety requirements list that must be met to call the EUC safe. The aspect *safety architecture* falsifies hypothesis H1.2 if no architecture can be found that reduces the identified risks to an acceptable level.

5 Research Tools

Section 5.1 of this chapter describes the synthetic and representative test manoeuvres that are used in the falsification experiments of the wheeled mobile platform, followed by a description of the virtual prototype (section 5.2) that is used for extrapolating the falsification experiments. Section 5.3 describes the measurement technology used with MORPHEUS and how signals are processed and is adopted from Wagner et al.[140].

5.1 Test Manoeuvres

Synthetic and representative test manoeuvres are used within this thesis, depending on the research aim. All experiments are carried out on the August-Euler-Airfield in Darmstadt.

5.1.1 Synthetic Manoeuvres

Here, only those synthetic manoeuvres that are required for conducting experiments and simulation runs are described. The justifications for the choice of these manoeuvres are given in the sections where they are applied. Synthetic manoeuvres are artificially generated and, therefore, the input signals are noise-free. All synthetic manoeuvres are driven without washout and TC. For the 90° turn and the figure eight, scaling is applied in the MCA when necessary.

5.1.1.1 Straight-Line Acceleration

This manoeuvre is used for the verification of the power demand and the determination of the electric drive motor's and its motor controller's electrical efficiency that is used in the power/energy model. A longitudinal acceleration step input of constant amplitude is imposed to the DS at standstill up to its maximum velocity.

5.1.1.2 Steering Angle Step Input

A 90° steering angle step input is imposed to the DS, whereas the driving velocity may be varied. This manoeuvre is used for the determination of ACL.

[140] Wagner, P. et al.: Power, Energy, and Latency Test Drives with MORPHEUS (2017).

5.1.1.3 Perpendicular Acceleration Step Input

An acceleration step input is imposed to the DS, whereas the initial, perpendicular driving velocity may be varied. The acceleration step input amplitude may be varied, too. This manoeuvre is used for the determination of ACL.

5.1.1.4 90° Turn

The 90° turn (a.k.a. T-junction) is approached with 14 m/s. Then the vehicle is decelerated with 3 m/s² down to 5 m/s. As soon as the target velocity is reached, cornering is initiated with constant velocity. The cornering radius is 10 m. After a change in orientation of 90° has been reached, the vehicle accelerates with 3 m/s² to 14 m/s. The resulting acceleration, velocity, and yaw profile is processed in the MC (no washout and TC) and scaled if necessary[141a]. This manoeuvre is used to verify the energy model.

5.1.1.5 Figure Eight

The Figure eight manoeuvre is originally intended to evaluate the control and tire behaviour. It is driven at a constant longitudinal velocity of 1.5 m/s, whereas the heading of the WMDS follows the trajectory, i.e. with yaw. The cornering radius is 7.5 m, resulting in a maximum lateral acceleration of ±0.3 m/s². The resulting acceleration, velocity, and yaw profile is processed in the MC (no washout and TC) and scaled if necessary[141b]. This manoeuvre is used to verify the energy model.

5.1.2 Representative Manoeuvres

Graupner has developed a representative urban driving circuit that is composed of manoeuvres in a probabilistic distribution as they can be found in real urban driving[142]. Four different drivers that were familiar with the driving circuit drove the measurement runs during the day, off-hour, resulting in an above-average performance compared to normal drivers. The car used was a VW Golf VI R, equipped with a GeneSys ADMA G-3 measurement unit, logging translational accelerations and rotational velocities at a sampling rate of 100 Hz. The circuit is about 21 km long and takes about one hour to complete[141c,143]. The urban measurement runs are used for the evaluation of the energy demand, where MORPHEUS must represent the recorded accelerations.

Because the measured acceleration and velocity signals are prone to sensor noise and vibration induced from the test vehicle, filtering is applied. The reason is that in a real DS application the control inputs for the MCA are firstly generated by the driver through the

---

[141] Cf. Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). a: pp. 90f.; b: pp. 91ff.; c: pp. 93f.

[142] Graupner, M.: Bachelor's thesis, Entwicklung eines repräsentativen Stadtparcours (2011).

[143] Betz, A. et al.: Motion Analysis of a WMDS (2012).

HMI (steering wheel angle, pedal positions) and secondly transformed to translational accelerations and rotational velocities in a vehicle model. The resulting accelerations and velocities are free of measurement noise so that the application of noisy data from the urban measurement runs would misrepresent the demand upon the MCA.

When modelling a vehicle, frequencies below 8 Hz typically characterise the vehicle behaviour (driving test support, control system design), whereas frequencies between 3 Hz and 20 Hz characterise handling (vehicle dynamics, driving stability), and everything above 8 Hz is relevant for comfort analysis (comfort and vibration analysis, durability profiles)[144]. Therefore, a Finite Impulse Response (FIR) low-pass filter is applied, whereas the passband frequency is chosen to 8 Hz and the stopband frequency to 10 Hz (comfort is not of interest). A Kaiser window is used. Figure 5-1 shows the Power Spectral Density (PSD) for the unfiltered (left) and filtered (right) longitudinal acceleration signal of urban measurement run 2:

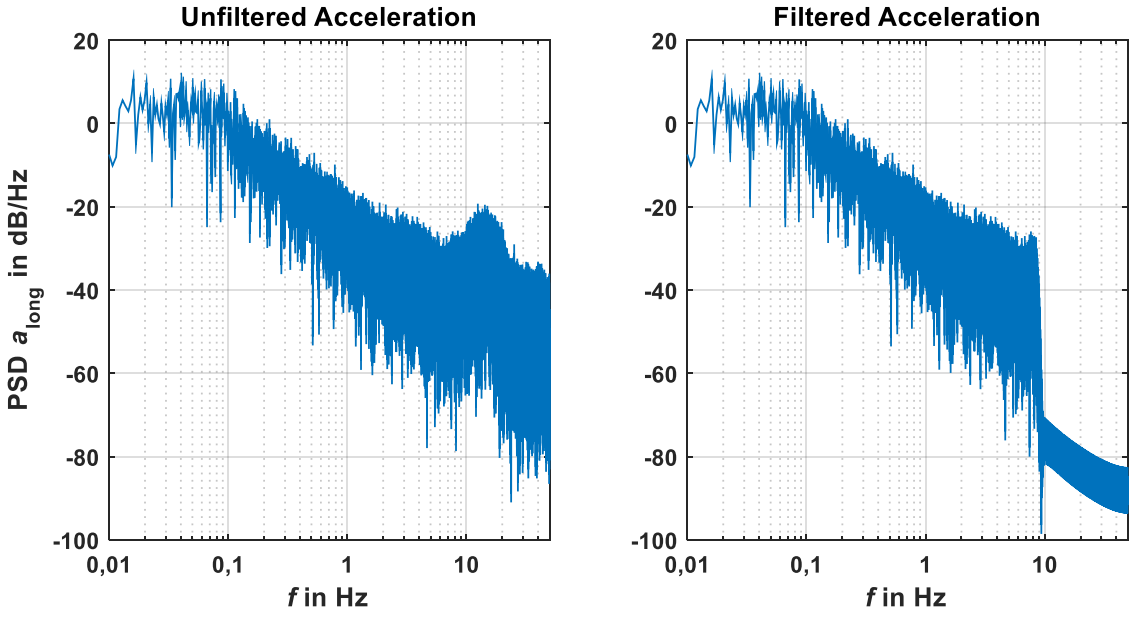

Figure 5-1: PSD of the discrete Fourier transform of the longitudinal acceleration signal of urban measurement run 2. Left: Unfiltered acceleration signal, right: Low-pass filtered acceleration signal.

[144] Ammon, D.; Schiehlen, W.: Advanced Road Vehicles: Control Technologies (2009). p. 285.

5.2 Virtual Prototype

A virtual prototype is available, programmed in MATLAB Simulink and IPG CarMaker. The MCA and MC are identical to those of MORPHEUS. IPG CarMaker simulates the driving dynamics with a frequency of 1 kHz. The virtual prototype is used for scaling the measured energy demand of MORPHEUS in a downscaled urban driving scenario up to that of an unscaled urban driving scenario. The CarMaker model is required for these simulations because of its sophisticated tire model.

5.2.1 Tire Model[145,146]

The press-on band tires are modelled based on Pacejka's fully non-linear single contact point transient tire model combined with the Magic Formula 5.2 and is accessed through the Simulink interface of CarMaker. The parameters are derived from measurements of the tire's longitudinal and lateral friction coefficient, and lateral force in dependence on the slip angle. The drill torque $T_{\mathrm{drill},i}$ and the self-aligning torque $T_{\alpha,i}$ were empirically determined in dependence on turn slip and slip angle, respectively, and are then provided by the magic formula. The model has been validated[147].

5.2.2 Body Model[148]

The body is modelled in CarMaker with point masses. Because CarMaker is intended for passenger cars, the body model consists of four wheels. For applying the model to the three-wheeled WMDS concept, the fourth wheel is minimised in size and mass and has no ground contact. The geometric properties of section 3.6 are applied.

---

[145] Cf. Zöller, C. et al.: Tire Concept Investigation for WMDS (2016).

[146] Cf. Zöller, C. et al.: Tires and Vertical Dynamics of WMDS (2017).

[147] Zöller, C.: Master's thesis, Implementierung und Parametrierung eines Reifenmodells für WMDS (2014).

[148] Cf. Betz, A. et al.: Driving Dynamics Control of a WMDS (2013).

5.2.3 Chassis Model[149]

The MORPHEUS prototype has no chassis, i.e. chassis properties like camber, kingpin inclination, toe and offset are zero. The steering angle is infinite. In addition, the properties remain unchanged during wheel lift. All this is accounted for in the CarMaker chassis model. Because of numerical problems, the damping constant and the spring stiffness of the chassis cannot be set to infinity but are iteratively maximized to values of 2.5 kNs/m and 25 kN/m respectively, to minimize their influence on the virtual prototype's dynamic behaviour.

5.2.4 Power/Energy Model[150]

Energy is demanded by electric and electronic components. These components can be divided into motion simulation components that must be supplied with energy for moving MORPHEUS (electric motors and motor controllers, hexapod's linear actuators and power electronics) and into auxiliary simulation components that do not actively contribute to motion simulation but are necessary for control (e.g. IPG Roadbox, ADMA G-3, simulation computers, etc.). The auxiliary component's power demand is assumed to be nearly constant. Therefore, their demand can be measured (cf. section 6.3.2) and easily modelled. The motion simulation components, on the other hand, show a strongly velocity- and load-dependent behaviour, which makes it necessary to identify and model the driving resistances as well as the behaviour of the electric components. Recuperation is accounted for in the model, although not separately modelled: If the demanded wheel hub torque becomes negative, energy is recuperated with the same efficiency as when energy is drawn from the accumulator. Still, in experiments, recuperation's influence on the overall energy demand was marginal. The integration of the steering and drive power demand over time yields the total energy demand of MORPHEUS. The output current and voltage of the High Voltage (HV) accumulator are measured in the experiments. Therefore, an ideal (i.e. $\eta_{\text{accumulator}} = 1$) accumulator model is used. Figure 5-2 gives an overview of the energy model and its interaction with other submodels, whereas the description of the model is given in the following subsections:

---

[149] Cf. Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 112.

[150] Cf. Albrecht, T. et al.: Advanced Design Project, Fahrwiderstands- und Energiebedarfsbetrachtung des MORPHEUS (2016).

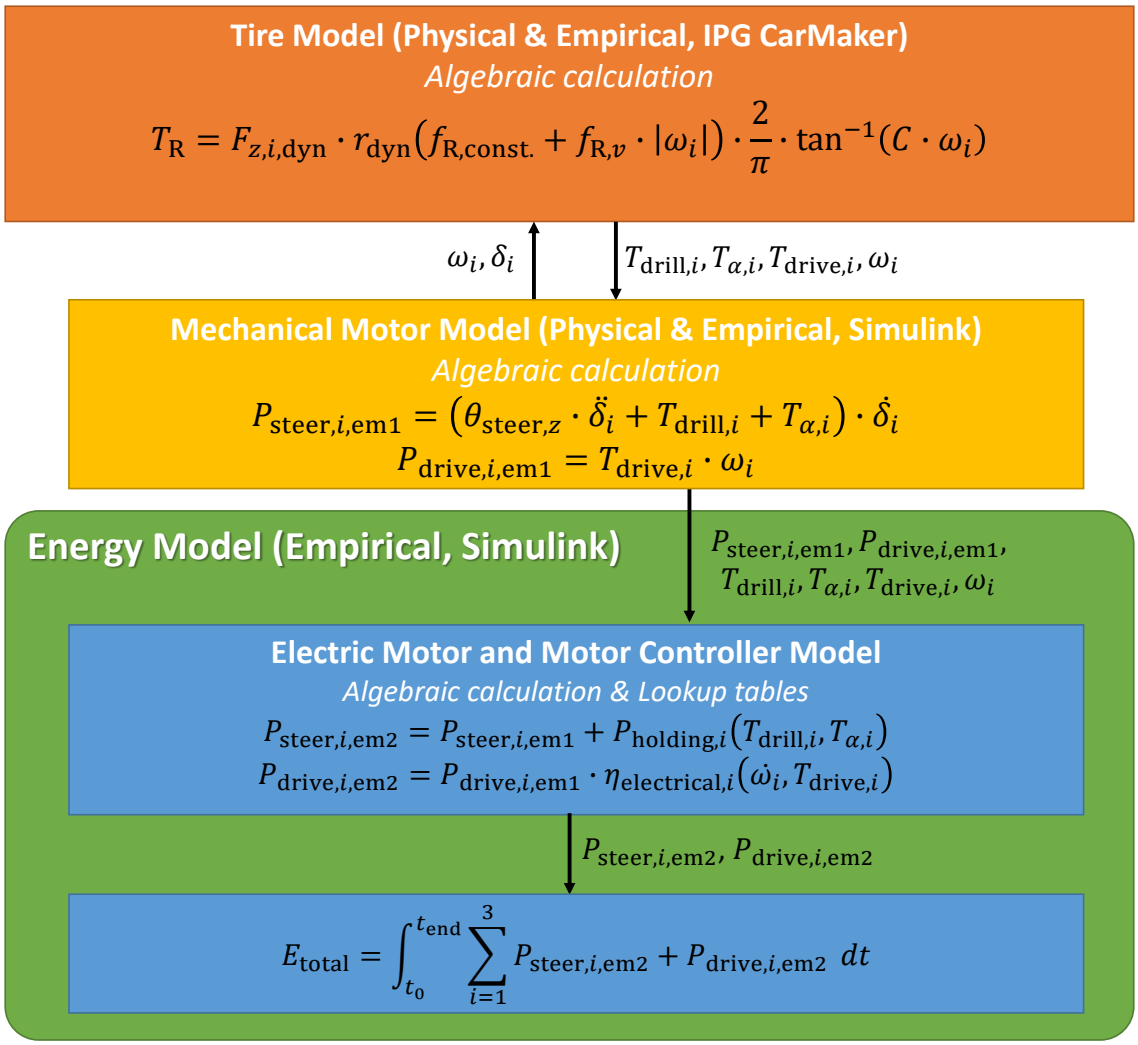

Figure 5-2: MORPHEUS' energy model

5.2.4.1 Drive Units' Driving Resistances

Climbing resistance (even driving surface) and rolling resistance because of the displacement of water (MORPHEUS must not be used under wet weather conditions) can be neglected. Furthermore, and as expected, test drives have shown that **air resistance** (a.k.a. drag) has no significant influence on the overall driving resistance (velocity shows no quadratic dependence on time when coasting)[151]. Thus, air resistance is neglected, also because the maximum velocity of MORPHEUS is just slightly above 10 m/s and about 90 % of all unscaled driving manoeuvres are representable with a maximum velocity of 8.5 m/s[152]. This simplification must be re-evaluated when using a full-scale WMDS with

[151] Albrecht, T. et al.: Advanced Design Project, Fahrwiderstands- und Energiebedarfsbetrachtung des MORPHEUS (2016). p. 32.

[152] Betz, A. et al.: Motion Analysis of a WMDS (2012).

a dome. In addition, energy dissipation in the **suspension** is neglected, because no dampers are used in the chassis and the influence of tire damping is not significant. **Slip losses** are accounted for in the validated tire model. The **acceleration resistance** including the equivalent mass of rotating parts e_m is included in IPG CarMaker. The CarMaker model is parameterised with geometric relations, masses, and mass moments of inertia, which are either determined in experiments or derived from the verified CAD model[153]. The **rolling resistance** coefficients are determined in coasting experiments (cf. section 6.1.1.1) and integrated into the tire model in IPG CarMaker. By coasting with switched-off drive motors, the **drive unit's friction** (actually a drivetrain loss) influences the rolling resistance as well as the **air resistance**, which is not modelled separately. Thus, a general driving resistance with linear dependency on velocity is determined and denominated with the index R.

5.2.4.2 Drive and Steering Units' Mechanical Motor Model

The mechanical motor model is provided with wheel speed as well as demanded wheel hub and steering torque from the IPG CarMaker model and is not part of the actual energy model. Nevertheless, it is important to understand how the steering and drive power are calculated and forwarded to the energy model. The mechanically required steering power is calculated by multiplying the sum of the torque required to overcome the moment of inertia, the drilling torque, and the self-aligning torque with the steering angle rate. The axial mass moment of inertia (including wheel, drive unit, parts of the gearbox and slip ring, etc.) is determined with a fully parameterised CAD model that has been verified to be sufficiently accurate[153]. The drilling and self-aligning torque are provided by the tire model, which has been validated[154]. Multiplying the provided wheel speed and demanded wheel hub torque yields the mechanically required drive power.

5.2.4.3 Steering Units' Electric Motor and Motor Controller Model

For the steering motors, the holding power is added to the mechanically required steering power. The holding power results from the control effort of the motor and its controller – especially when cornering – and is determined in experiments (cf. section 6.1.1.2).

5.2.4.4 Drive Units' Electric Motor and Motor Controller Model

Initially, the electric drive motor model was based on an efficiency map provided by the manufacturer, plotting the relative efficiency over motor speed and torque. The motor controller was modelled, in consultation with the supplier, with a constant efficiency of 95 %. Unfortunately, simulation results showed a large discrepancy to MORPHEUS'

[153] Wagner, P.: Master's thesis, Aufbau und Inbetriebnahme eines WMDS (2013).

[154] Zöller, C.: Master's thesis, Implementierung und Parametrierung eines Reifenmodells für WMDS (2014).

measured energy demand, which is why the decision was made to determine a joint efficiency model for the electric motor and its motor controller. For highest accuracy, experiments on a test bench would be required that was not available. Thus, constant acceleration experiments with varying acceleration amplitudes were conducted. Dividing the mechanically required power, calculated from the motion quantities measured by the ADMA G-3 and the previously determined driving resistance and steering holding power, by the actual required electrical power yields the overall efficiency of the system for all points of operation.

5.3 Measurement Technology

Motion quantities are measured by

- three fibre-optic gyroscopes: angular velocities,
- three inertial sensors: linear accelerations,
- and a GPS/DGPS receiver: 3D position and velocity,

and are merged and filtered into an overall 3D motion information by a GeneSys ADMA G-3. Motor resolvers measure the electric motors' position that is transferred to the motor controllers from where these values are tapped together with the signal of a current sensor that is positioned between each electric motor and its motor controller. Another current and voltage sensor is installed at the main accumulator for identifying the peak power and average energy demand. Acceleration as well as rotational and translational velocity are measured with 1 kHz, current as well as voltage of the main accumulator with 200 Hz (limited by sensor), and motor currents and revolutions with 100 Hz (limited by sensors). Sensor noise, vibrations of the electric motors, and body vibration due to vertical excitation from the road surface cause signal disturbance. The PSD of the discrete Fourier transform of a longitudinal acceleration signal is shown in Figure 5-3.

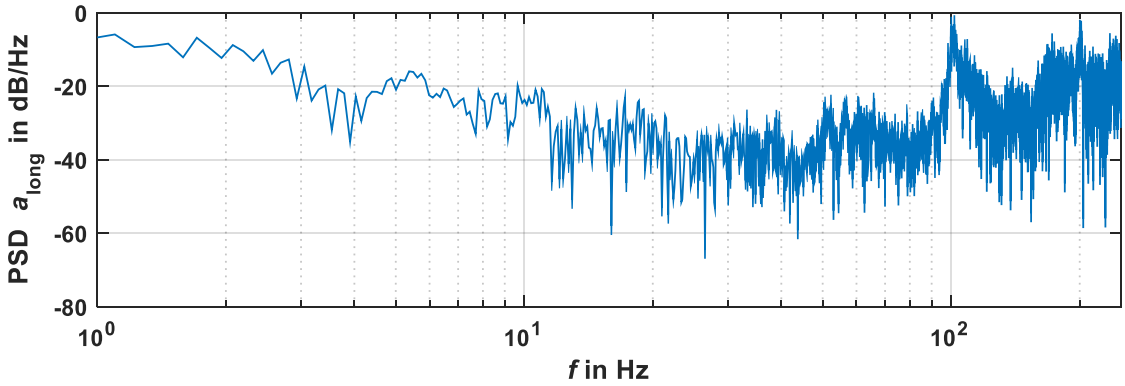

Figure 5-3: PSD of discrete Fourier transform of longitudinal acceleration signal for a 90° steering angle input at v_{long} = 2 m/s, trial 1)

Therefore, acceleration signals are low-pass filtered in the same manner as for the urban measurement runs in section 5.1.2. In accordance with the values found from literature (section 5.1.2) a finite impulse response (FIR) low-pass filter with a passband frequency of 7 Hz and a stopband frequency of 13 Hz is chosen. A Kaiser window is used. Figure 5-4 shows the comparison between the unfiltered (orange dots) and low-pass filtered (yellow line) measured longitudinal acceleration signal.

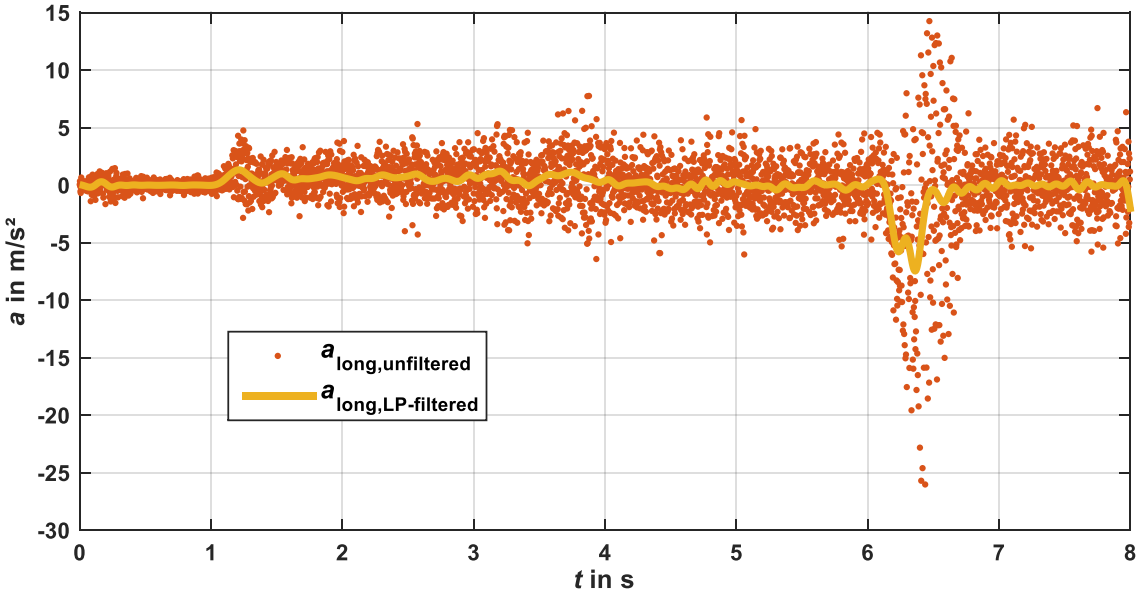

Figure 5-4: Comparison of unfiltered and low-pass filtered measured longitudinal acceleration (90° steering angle input at v_{long} = 2 m/s, trial 1)

The reason for the noisy acceleration signals can be found in the vertical excitation due to the road surface, which is a major problem at the current state of research. A normalized cross-correlation of the vertical and longitudinal acceleration signal from the same test drive as in Figure 5-4 is calculated and plotted in Figure 5-5. The lateral and vertical acceleration signals are dependent on each other between ±200 ms lag, whereas the lateral acceleration signal follows the vertical acceleration signal. This suggests an influence of vertical acceleration, and, therewith, vertical excitation, onto horizontal acceleration. Reducing the vertical excitation of MORPHEUS' self-driving platform is expected to reduce acceleration signal disturbance and to improve the tires' force transmission potential at increased velocities.

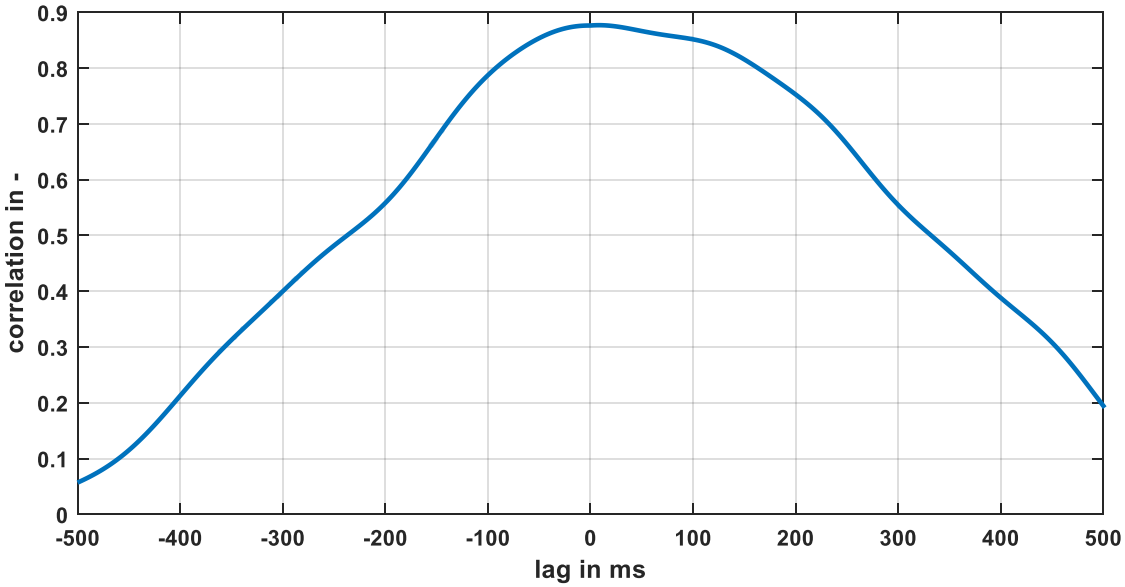

Figure 5-5: Normalized cross-correlation of equally low-pass filtered vertical and lateral acceleration signal (90° steering angle input at v_{total} = const. = 2 m/s, trial 1, from manoeuvre initiation to end of manoeuvre (i.e. $a_{\text{lat}} > 0$))

6 Falsification Experiments for Wheeled Motion Base

Initially, the power/energy model, its parameterisation, and its verification/validation are described (section 6.1). The model is used to extrapolate the results of the energy demand experiments to unscaled driving manoeuvres and to investigate the power demand in dependence of the scaling factor. Section 6.2 provides the results for the power demand falsification experiments, section 6.3 for the energy demand falsification experiments, and section 6.4 for the motion latency falsification experiments. A summary and an outlook to the application of the found results and used methodology in unscaled WMDS will be given at the end of each of these sections. The results described in sections 6.1.2.2, 6.3, and 6.4 are adopted from Wagner et al.[155].

6.1 Power/Energy Model

6.1.1 Parameter Identification

6.1.1.1 Drive Units' Driving Resistance (Coasting Tests)[156]

To determine the driving resistance coefficient, MORPHEUS is accelerated inside a hangar to a velocity of 3.6 m/s. Thus, interferences due to wind are eliminated. After reaching the desired velocity, the drive motors are switched off and the WMDS coasts into standstill. Acceleration and velocity are continuously measured with the ADMA G-3, supported by a Correvit (GPS is not available inside the hangar), and filtered. The experiment is carried out 15 times in each direction, thus, influences from climbing resistance are eliminated, totalling in 30 runs. Then, all acceleration and velocity signals are shifted so that 0.2 m/s are reached simultaneously. Finally, the signals are averaged overall all trials. Figure 6-1 shows the averaged acceleration over velocity. This a vs. v presentation is chosen over the traditional a vs. v^2 presentation as it is used in coasting tests with passenger cars, because a linear relation between deceleration and velocity is identified in the experiments. This can be explained with the low velocities driven and the negligible (quadratic) influence of air resistance.

[155] Wagner, P. et al.: Power, Energy, and Latency Test Drives with MORPHEUS (2017).

[156] Cf. Albrecht, T. et al.: Advanced Design Project, Fahrwiderstands- und Energiebedarfsbetrachtung des MORPHEUS (2016).

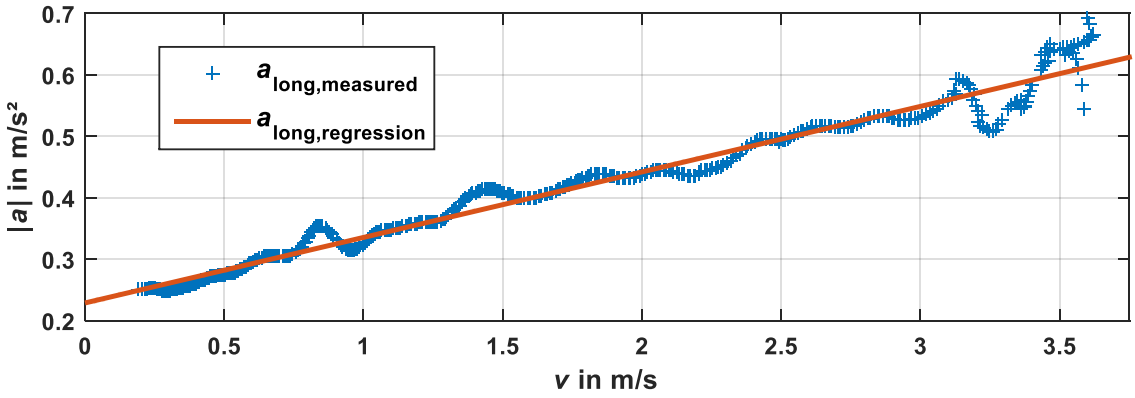

Figure 6-1: Absolute deceleration over velocity in coasting experiments (averaged over all trials)

A linear regression of the form of equation (6-1) is fitted to the a vs. v diagram in Figure 6-1, from which can be concluded that a constant and a linearly velocity-dependent driving resistance coefficient may be approximated. The regression yields the constant driving resistance coefficient that can also be read from the intersection point with the ordinate in Figure 6-1, equation (6-2):

$$a_{\text{regression}} = g \cdot \left(f_{\text{R,const.,regression}} + f_{\text{R},v,\text{regression}} \cdot \frac{v}{r_{\text{dyn}}} \right) \tag{6-1}$$

$$\rightarrow f_{\text{R,const.,regression}} = 0.0233 \tag{6-2}$$

The constant driving resistance coefficient is about 2.5 times the rolling resistance coefficient that can be found on passenger cars with pneumatic tires. For the velocity-dependent driving resistance coefficient, the slope of the linear regression is used, equation (6-3):

$$\rightarrow f_{\text{R},v,\text{regression}} = 0.0015 \ \frac{\text{s}}{\text{rad}} \tag{6-3}$$

It must be stressed again that these coefficients do not solely represent the rolling resistance but also include air resistance and friction in the drive units. The driving resistance is implemented in the tire model. Given the omnidirectionality of the concept, the wheels can turn in both directions at all velocities, making it necessary to implement the driving resistance for both directions of rotation. Using a signum function is numerically critical, which is why the decision was made for the arc tangent, wherein C is a parameter to design the shape of the imitated signum function. Figure 6-2 shows the resulting driving resistance torque plotted over the wheel speed in dependence on the parameter C.

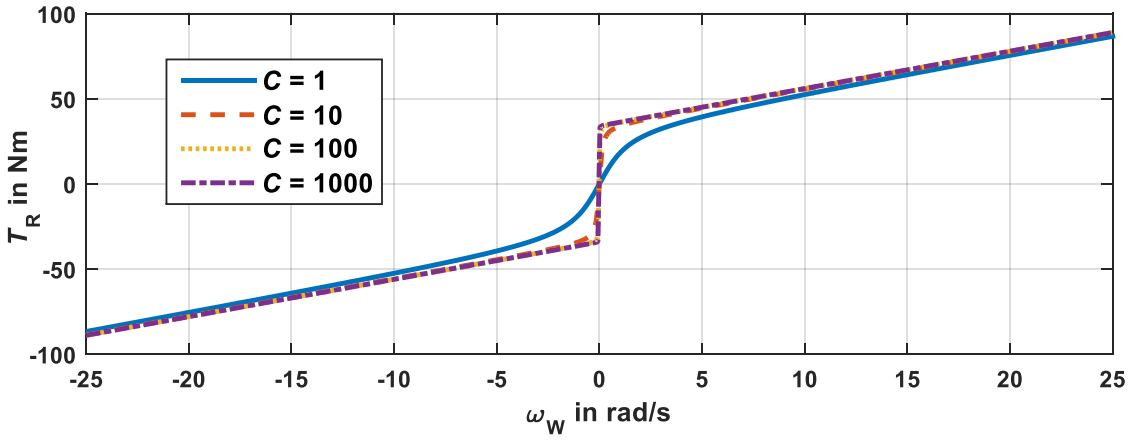

Figure 6-2: Driving resistance torque over wheel speed in dependence on parameter C

From the diagram can be concluded that values larger than 100 provide the best approximation to a signum function. Therefore, C is set to 1,000. Thus, the formula for the driving resistance at each wheel is:

$$T_{\mathrm{R},i} = F_{z,i,\mathrm{dyn}} \cdot r_{\mathrm{dyn}} \left(0.0233 + 0.0015 \frac{\mathrm{s}}{\mathrm{rad}} \cdot \left|\omega_{\mathrm{W},i}\right|\right) \cdot \frac{2}{\pi} \tan^{-1}\left(1{,}000\ \omega_{\mathrm{W},i}\right) \tag{6-4}$$

6.1.1.2 Steering Units' Electric Motor and Motor Controller Model (Holding Torque Test)[157a]

To determine the holding torque, an external tangential force is applied to a drive motor while the tire has no contact to the underground. A torque sensor mounted to the steering unit measures the supporting torque provided by the steering motor. The steering angle is controlled to stay constant, Figure 6-3.

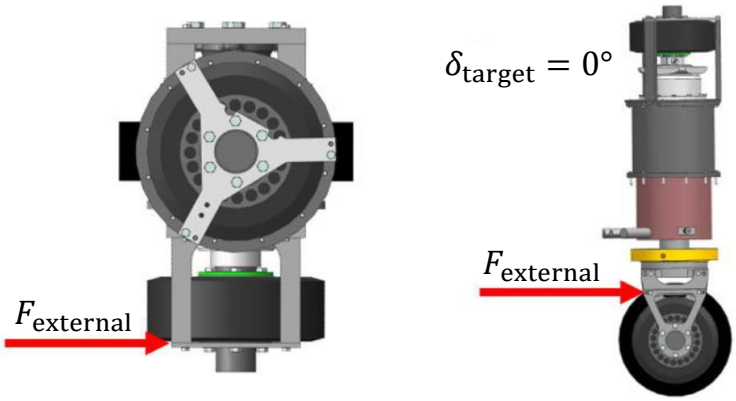

Figure 6-3: Experiment setup for holding torque test[157b]

[157] Cf. Albrecht, T. et al.: Advanced Design Project, Fahrwiderstands- und Energiebedarfsbetrachtung des MORPHEUS (2016). a: - ; b: p. 41.

The external force is increased incrementally up to a resulting holding torque of 50 Nm, whereas each increment is applied several times for the sake of reproducibility. The traction battery's output current and voltage are measured. Figure 6-4 shows the measured steering power plotted over the measured holding torque for one steering motor.

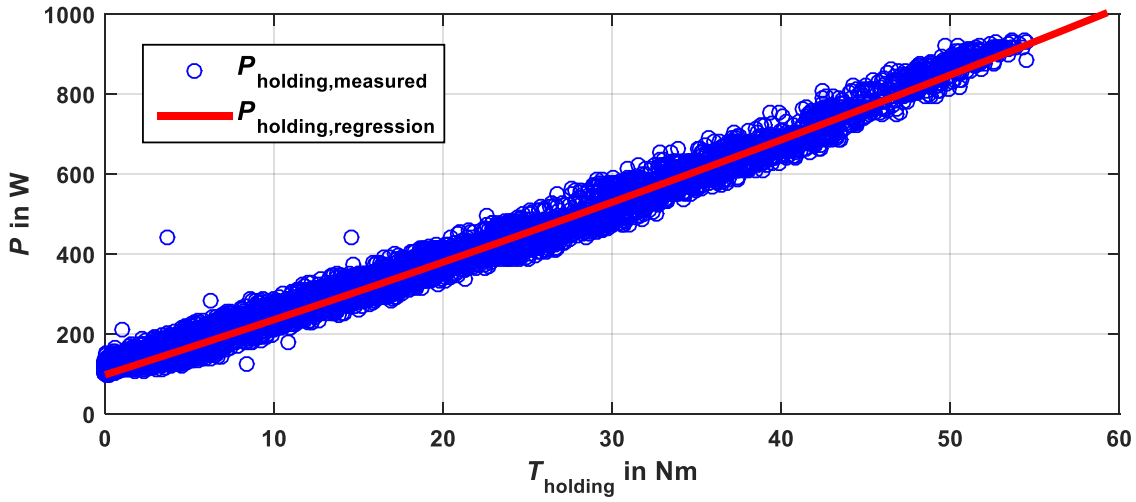

Figure 6-4: Measurement data and regression for holding torque[158]

A quadratic regression is fitted, whereas the offset of 97.5 W arises due to the control effort for keeping the steering angle constant:

$$P_{\text{holding},i} = 0.03\,\frac{1}{\text{Nms}} \cdot T_{\text{holding},i}^2 + 13.5\,\frac{1}{\text{s}} \cdot T_{\text{holding},i} + 97.5\ \text{W} \tag{6-5}$$

6.1.1.3 Drive Units' Electric Motor and Motor Controller Model (Constant Acceleration Test)

Straight-line acceleration tests are driven with MORPHEUS. The acceleration amplitude is varied from 0.2 m/s² to 7.2 m/s², whereas the increment is increased by 0.2 m/s² after each experiment since lower accelerations are driven more often. Because of the limited driving area and the required braking distance, the maximum velocity is reduced for the experiments with lower acceleration amplitude. Thus, the experiment setup as described in Table 6.1 was used.

Table 6.1: Experiment setup for constant acceleration tests

Experiment	#1	#2	#3	#4	#5	#6	#7	#8
a_{target} in m/s²	0.2	0.6	1.2	2	3	4.2	5.6	7.2
$v_{\text{target,max}}$ in m/s	6	8	10	12	12	12	12	12

[158] Albrecht, T. et al.: Advanced Design Project, Fahrwiderstands- und Energiebedarfsbetrachtung des MORPHEUS (2016). p. 42.

Acceleration and power signals are filtered and averaged over 30 trials that were conducted for each experiment. The electrical power drawn from the accumulator is the product of measured output current and output voltage of the accumulator. The mechanical power needed for horizontal acceleration is corrected by the driving resistance, the mass moment of inertia of the drive units, and the energy demand of the HV steering system. The constant HV energy demand of the steering units results from the required holding power (cf. section 6.1.1.2). Thus, the mechanically needed power is calculated to:

$$\begin{aligned} P_{\text{mech}} &= v \cdot \left(m \cdot \left(a + g \cdot \left(f_{\text{R,const.}} + f_{\text{R},v} \cdot \frac{v}{r_{\text{dyn}}} \right) \right) + \theta_{yy,\text{drive}} \cdot \frac{a}{r_{\text{dyn}}^2} \right) \\ &\quad + P_{\text{holding}}(0) \\ &= v \cdot \left(1{,}056\ \text{kg} \cdot \left(a + 9.81\ \frac{\text{m}}{\text{s}^2} \cdot \left(0.0233 + 0.0015\ \frac{\text{s}}{\text{rad}} \cdot \frac{v}{0.14\ \text{m}} \right) \right) \right. \\ &\quad \left. + 0.985\ \text{kgm}^2 \cdot \frac{a}{(0.14\ \text{m})^2} \right) + 292.5\ \text{W} \end{aligned} \tag{6-6}$$

The efficiency of the electrical components is then calculated by equation (6-7):

$$\eta_{\text{el}} = \frac{P_{\text{mech}}}{P_{\text{el}}} \tag{6-7}$$

Figure 6-5 shows the resulting efficiency map:

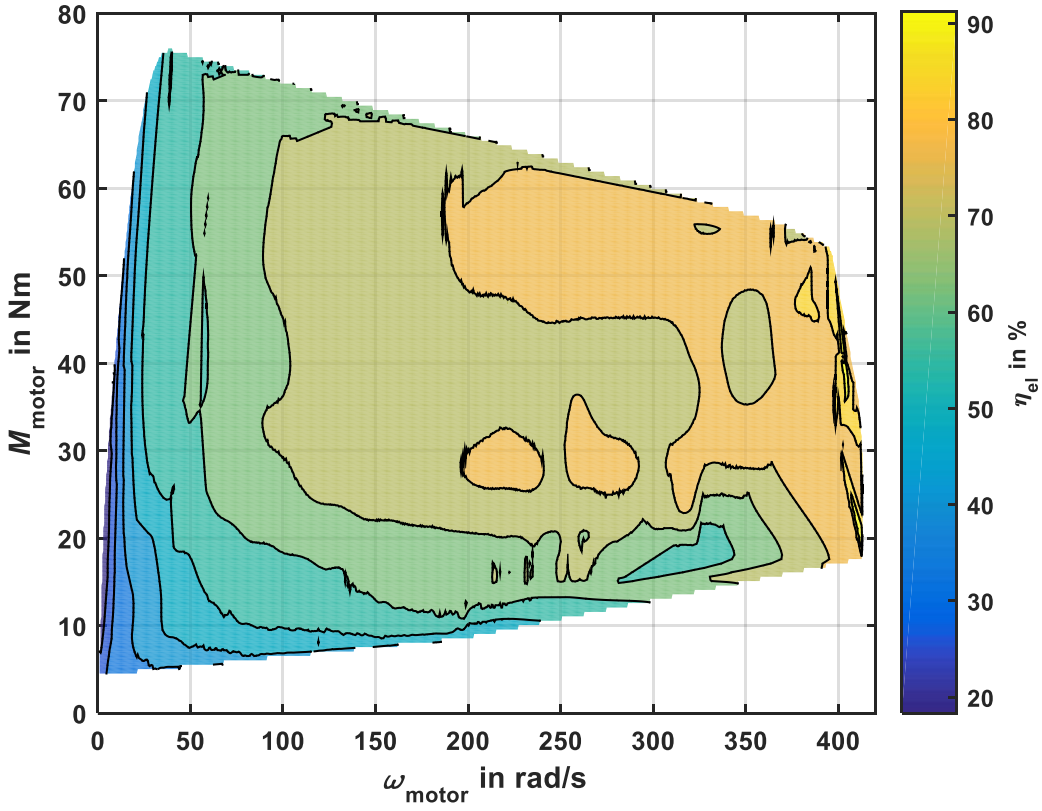

Figure 6-5: Efficiency map of drive unit's HV components

A comparably low efficiency of under 40 % is determined at low velocities. A low motor torque also has a significant influence on efficiency (under 60 %), although the influence is less than with velocity. The highest efficiency is reached at high motor speed and torque (proportional to velocity and acceleration). These observations coincide with data provided by Enstroj for the EMRAX 228 electric motor that is used on MORPHEUS (cf. annexe B.1). High accelerations could not be reached at high velocities. This issue will be discussed in section 6.2 where the power demand of MORPHEUS is investigated. The efficiency map is extrapolated with the nearest neighbour method, saved in a lookup table, and provided to the energy model. The extrapolation is not very accurate, but necessary because some operating points may lie outside the domain of the efficiency map. Still, the influence is expected to be negligible, because – as Betz[159] showed – 90 % of all situations in an unscaled urban driving scenario driven with the unscaled WMDS require no accelerations above 2.3 m/s² and no velocities above 7.5 m/s.

6.1.2 Verification/Validation

The power model is verified by comparing the power calculated by the model with the power measured in equivalent driving experiments, section 6.1.2.1. Basically, the energy model is the power model integrated over time. It is validated by conducting different types of manoeuvres and again comparing simulation and measurements, section 6.1.2.2.

6.1.2.1 Power Model Verification

Because the purpose of the power model is to investigate the maximum power consumption in a straight-line driving manoeuvre, the same manoeuvre is used for the verification. 50 data sets were recorded separately from the data sets used to parameterize the model. Figure 6-6 shows the resulting measured acceleration (blue stars), target acceleration (red line), measured velocity (yellow dots), measured power demand from the accumulator (violet circles), and the simulated electric power demand (green dashed line):

[159] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 108.

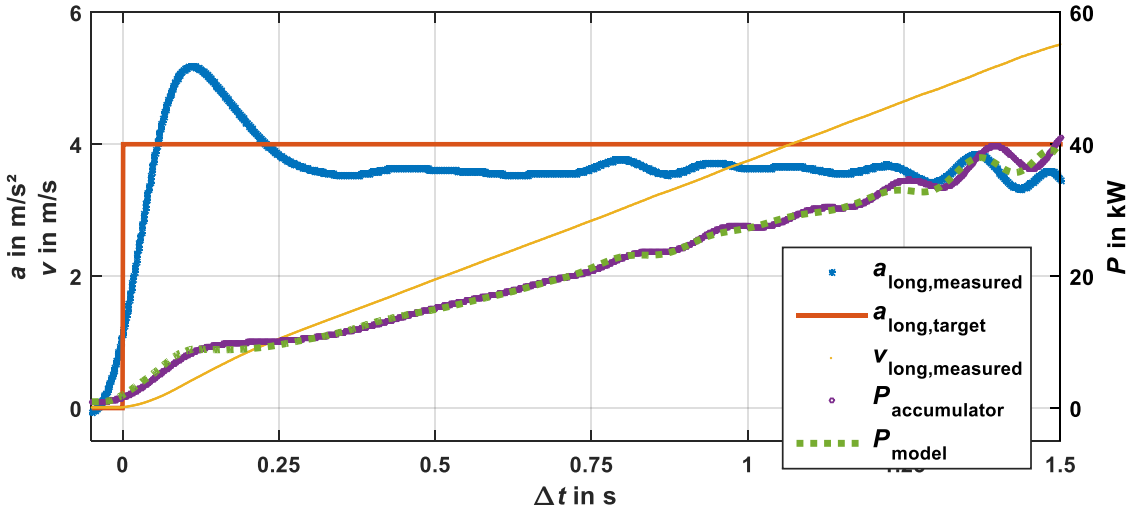

Figure 6-6: Verification of power model with 4 m/s² constant target acceleration manoeuvre (averaged over 50 trials)

The simulation matches the measurement. When jerking, the change in power demand occurs earlier in simulation than in the measurements, because the transient behaviour of the electric motors and motor controllers is not accounted for in the model. Still, these deviations are marginal and, therefore, the power model is sufficiently accurate for the purpose of simulating the power demand at higher accelerations and velocities.

6.1.2.2 Energy Model Validation

A bottom-up methodology is used for the validation of the energy model, starting with a simple 90° turn manoeuvre (averaged over six trials), then evaluating a figure eight manoeuvre (averaged over six trials), and ending with a complex ten minutes urban driving scenario (scaling factor 0.3, scenario #3, averaged over ten trials). Table 6.2 shows the virtual prototype's and MORPHEUS' energy demand during the manoeuvres, whereas σ is the standard deviation of and relative to the energy demand of the trials conducted with MORPHEUS.

Table 6.2: Results of the validation of the energy model

Manoeuvre	$t_{\text{manoeuvre}}$ in s	E_{sim} in Wh	E_{MORPHEUS} in Wh	σ_{MORPHEUS} in %	ΔE_{rel} in %
90° Turn	31	15.7	17	3.5	7.6
Figure 8	68	33.5	36	2.2	6.9
Urban (0.3 scaling)	600	360.8	358.8	4	0.6

The simulated energy demand of the synthetic manoeuvres undercuts the actual energy demand of MORPHEUS. In contrast, the representative urban driving circuit's energy demand is slightly higher in simulation than in reality. The deviation from the actual energy demand is around 7 % for the synthetic manoeuvres and 0.6 % for the scaled urban

driving circuit. Thus, the energy model may be used for estimating the platform's unscaled energy demand.

6.1.3 Adaption to Full-Scale WMDS

The power/energy model can be used for the full-scale WMDS, too, although a re-parameterisation will be required, because components like tires, bearings, electric motors, motor controllers, etc. will be changed. Furthermore, the influence of air resistance will become more significant as the maximum velocity will be increased. Therefore, the driving resistance should be modelled with a quadratic dependence on wheel speed. Nevertheless, the model structure as well as the methodology for parameterisation and verification can be kept. Therefore, an updated power/energy model for a full-scale WMDS can be made available in two or three working days, as soon as a working prototype is available. Then, the investigation of the falsification aspects can be conducted in the same manner as described within this thesis.

6.2 Power Demand

As previously stressed, the maximum velocity of MORPHEUS and the accumulator's output power are insufficient to conduct experiments for all occurring velocity amplitudes with scaling factors of up to 1. Therefore, the power/energy model is used to calculate the required mechanical and electrical power for representing the maximum acceleration and velocity amplitude of the corresponding scaling factor, equation (6-8):

$$\begin{aligned} P_{\mathrm{el}} &= \underbrace{\left(P_{\mathrm{R}} + P_{\theta_{yy}} + P_{\mathrm{steering}}\right)}_{P_{\mathrm{mech}}} \cdot \eta_{\mathrm{el}} \\ &= \Bigg(\Bigg(\Bigg(a + 9.81\ \frac{\mathrm{m}}{\mathrm{s}^2} \cdot \left(0.0233 + 0.0015\ \frac{\mathrm{s}}{\mathrm{rad}} \cdot \omega_{\mathrm{w}}\right) \Bigg) \\ &\quad \cdot 1{,}056\ \mathrm{kg} + 0.985\ \mathrm{kgm}^2 \cdot \frac{a}{(0.14\ \mathrm{m})^2} \Bigg) \cdot \omega_{\mathrm{w}} \cdot 0.14\ \mathrm{m} \\ &\quad + 292.5\ \mathrm{W} \Bigg) \cdot \eta_{\mathrm{el}}(\omega_{\mathrm{w}}, T_{\mathrm{mech}}) \end{aligned} \tag{6-8}$$

Figure 6-7 shows the result for this calculation, depicting the maximum output power of the accumulator (blue line) as well as the mechanically (yellow dotted line, including all

losses as described in sections 6.1.1.1 to 6.1.1.2) and electrically (red dashed line, including the electrical efficiency, equation (6-8)) required power for all maximum acceleration and velocity amplitudes of the corresponding scaling factor.

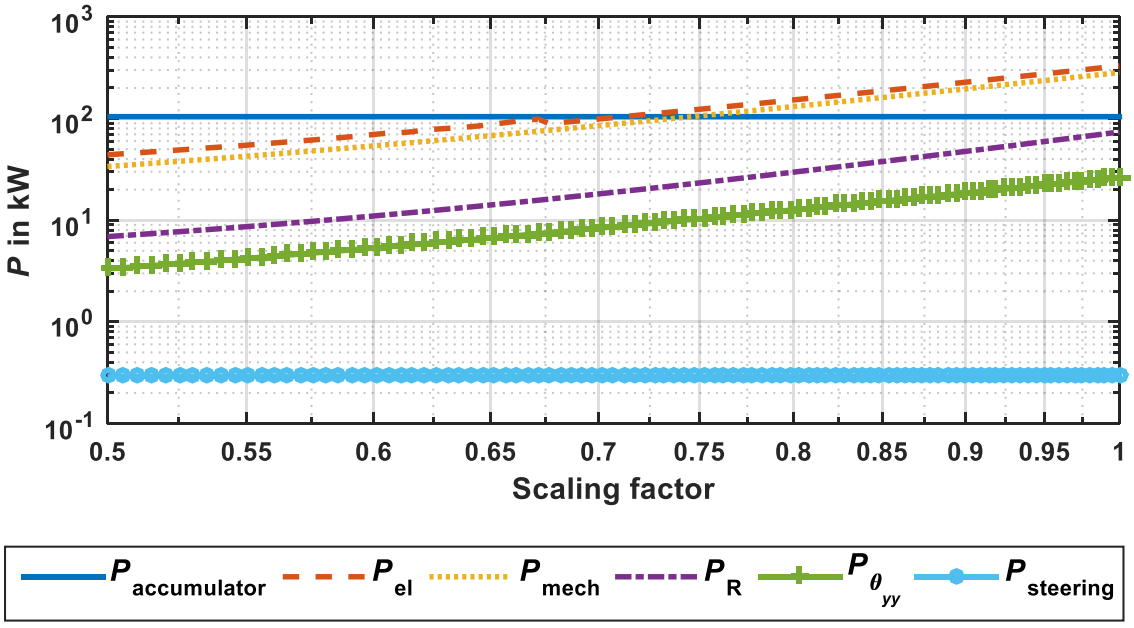

Figure 6-7: Power demand depending on the scaling factor (P_{steering} being the power required for steering, $P_{\theta_{yy}}$ being the power required for overcoming mass moment of inertia, P_{R} being the power required to overcome the driving resistances, P_{mech} being the sum of the three aforementioned powers, P_{el} being P_{mech} divided by the corresponding electrical efficiency yielding the required electrical power demand, and $P_{\text{accumulator}}$ being the power provided by the currently installed accumulator)

The electrical power demand can be fulfilled up to scaling factors of 0.7. At higher scaling factors, the power output of the accumulator is insufficient. A mechanical power of about 250 kW is sufficient for unscaled driving simulation, whereas – in this case – the electrical power drawn from the accumulator is less than 300 kW. The first requirement is already fulfilled by the built-in electric motors. The second requirement can be fulfilled by employing three accumulators instead of one. No conclusions can be drawn for the full-scale WMDS, because different electric motors and a more detailed design would be needed. Still, the found results increase the confidence in the feasibility of the aspect power demand.

Concluding, the aspect *power demand cannot falsify* hypothesis H1.1 when applying state-of-the-art accumulator and actuator technology.

6.3 Energy Demand

6.3.1 Motion Energy Demand (HV)

Four unscaled, representative urban driving scenarios (section 5.1.2) are simulated with the verified energy model of the virtual prototype and a WMDS mass of 1,302 kg (full setup, cf. section 3.6) to determine the maximum energy demand. The results are presented in Table 6.3, whereas the worst-case energy demand of urban driving scenario #1 will be used for the evaluation.

Table 6.3: Simulated energy demand for unscaled, representative, urban driving scenarios

Urban driving scenario #	t_{sim} in s	E_{sim} in Wh	$\emptyset P_{\mathrm{sim}}$ in W
1	3,500	10,908	11,220
2	3,100	9,185	10,666
3	2,900	7,700	9,559
4	3,500	7,999	8,228

Unfortunately, the hexapod was not operable and therefore no energy demand could be determined. Betz identified a Tripod's average power demand for tilt coordination in an unscaled, representative urban driving scenario simulation based on the actuators' lengths and velocities to be 32 W[160]. The average power required for holding the load was neglected in simulation but estimated to be 100 W[160]. Adding an estimate for the power electronics' average energy demand yields a total power demand of 200 W for the hexapod's TC task.

6.3.2 Auxiliary Energy Demand (LV)

A 12 V (DC) and a 24 V (DC) auxiliary electrical system with separate LV accumulators are used on MORPHEUS. Because the aim is to replace the LV accumulators with a DC/DC converter to solely use the HV accumulator, every auxiliary energy consumer's energy demand is measured in every possible operating state. Adding each consumer's maximum demand yields an overall worst-case power demand of 821.9 W, Table 6.4. Only the wireless emergency stops, the motor controllers, the power contactors, and the visual and audible representation system showed a significant increase in energy demand between idle and full operational:

[160] Betz, A. et al.: Motion Analysis of a WMDS (2012).

Table 6.4: Auxiliary consumers' maximum power demand

Auxiliary component	$P_{max,measured}$
IPG Roadbox	30.3 W
Wireless emergency stop	2.3 W
Programmable logic controller	3.5 W
Magnetic clamps (safety system)	121.7 W
Status LEDs	0.6 W
Wireless router	4.8 W
Motor controllers	78 W
Battery Management Systems (BMS)	4 W
Power contactors	3.6 W
ADMA G-3	18.1 W
Visual & audible representation system (comprised of four simulation computers, Oculus Rift + camera, two monitors for system operator, fan, mock-up illumination, speakers, and HMI)	555 W

6.3.3 Discussion

The worst-case average power demand for an unscaled, representative urban driving scenario is 12.2 kW (11,220 W platform, 200 W hexapod, 822 W LV), which results in an energy demand of 24.4 kWh for a 2 h simulation run. Thus, the initial requirement for the energy demand is not met for the currently installed accumulator (532.8 V · 10 Ah = 5.33 kWh). Nevertheless, adding four further HV accumulators (mass 34 kg each) is reasonable, especially if a DC/DC converter (e.g. Bel Power Solutions 700DNC40-12-xG with 4 kW output power[161], mass 22 kg) compensates for the four LV accumulators (mass approx. 20 kg each), resulting in an added net weight of 78 kg. Of course, the mass increase leads to an increase of the platform's power demand, yielding an updated **energy demand of 25.7 kWh for a 2 h simulation run, which can be fulfilled with the 26.6 kWh energy of five HV accumulators**. Also, the **power demand requirement can be fulfilled** with increased accumulator power.

Even when considering the energy demand for the 0.3 scaled urban driving scenario (section 6.1.2), a simulator runtime of 2 h 28 min is enabled with the current accumulator. If more demanding (i.e. more dynamic), manoeuvres are conducted, the average power demand is expected to increase, thus, decreasing the possible simulation duration. Recalling the reasoning for the 2 h test drive requirement, being that longer simulation exposures

[161] Bel Power Solutions: 700DNC40-12-xG DC/DC Converter Data Sheet (2017). p. 4.

increase the risk of simulator sickness (section 2.4), dynamically more demanding manoeuvres would increase the susceptibility to simulator sickness. Therefore, shorter possible experiment durations compensate for the increased energy demand.

Concluding, the aspect *energy demand cannot falsify* hypothesis H1.1 when applying state-of-the-art accumulator technology.

6.4 Acceleration Cue Latency

6.4.1 Variation of Acceleration Step Input Amplitude

Recalling the methodology for measuring latency (section 4.3.2), lateral acceleration signals are used for these experiments, whereas the results are evaluated with different criteria for lateral and longitudinal acceleration cue latency. Figure 6-8 describes the evaluation methodology by showing an exemplary lateral acceleration step input (red point-dashed line) and MORPEHUS' lateral acceleration response (blue stars). Additionally, the $IACL_{50\,\%}$ (i.e. 50 % of target acceleration, purple dashed line) and $IACL_{gain}$ (i.e. 0.2 m/s², black solid line) are shown.

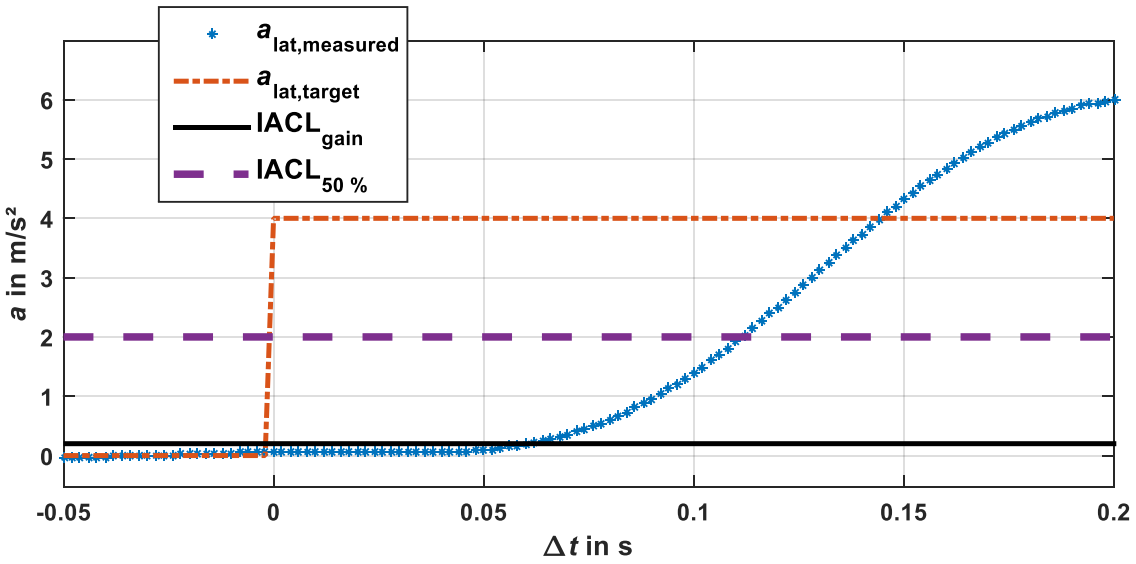

Figure 6-8: Exemplary acceleration time signals for a 4 m/s² lateral acceleration step input at 1 m/s longitudinal velocity (trial 1)

Fifty percent of the target acceleration is reached after approximately 110 ms and 0.2 m/s² are reached after approximately 60 ms for this exemplary test drive. The table with the detailed results can be found in annexe B.1, whereas Figure 6-9 gives a graphical overview:

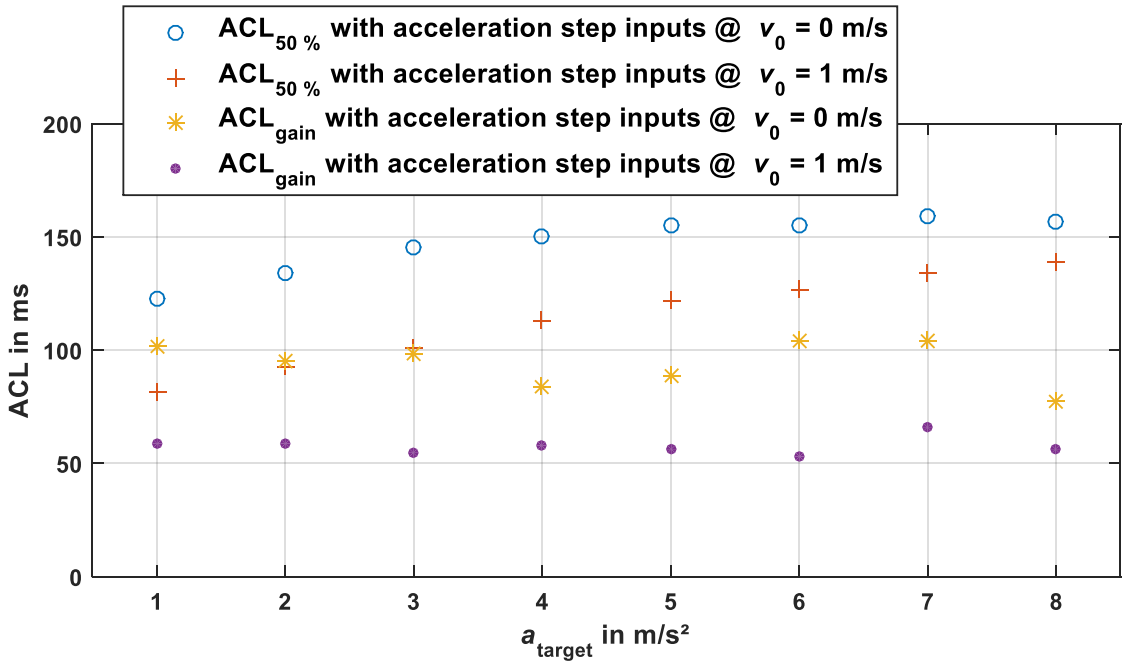

Figure 6-9: $ACL_{50\,\%}$ and ACL_{gain} caused by an acceleration step input with varied initial velocities of 0 and 1 m/s and varied acceleration step input amplitude (values are averaged over six trials)

The variation of the acceleration step input amplitude yields variable results for $ACL_{50\,\%}$, Figure 6-9, because the $IACL_{50\,\%}$ is slightly dependent on the step input amplitude itself. For example, in a trial with a step input of 2 m/s² amplitude, the latency measurement time ends as soon as 1 m/s² (=$IACL_{50\,\%}$) are measured, whereas with a step input of 8 m/s² amplitude, an acceleration of 4 m/s² must be measured. Thus, $ACL_{50\,\%}$ increases with the acceleration step input and reaches its maximum of 159 ms at 7 m/s² and 0 m/s. Still, the results are rather dependent on the $IACL_{50\,\%}$ than the input variation itself. The average of the relative Mean Standard Deviation (MSD) of each $ACL_{50\,\%}$ set of six trials (annexe B.1 and B.3) is 4.4 %, proving the robustness of the $IACL_{50\,\%}$.

As expected, for the constant acceleration threshold based ACL_{gain} can be stated that the acceleration step input amplitude has no major influence on latency. The relative MSD for the ACL_{gain} is 17.4 % for 0 initial driving velocity and 10.9 % for 1 m/s initial driving velocity, respectively. The maximum ACL_{gain} is reached at 6 and 7 m/s² and 0 m/s and is 104 ms. The average of the relative MSD of each ACL_{gain} set of six trials (annexe B.1 and B.3) is 14.6 %, showing that the $IACL_{gain}$ is more sensitive than the $IACL_{50\,\%}$.

Most important, an influence of the driving velocity on the ACL can be noted for both IACL, as ACL increases with decreasing driving velocity.

6.4.2 Variation of Initial Longitudinal Velocity

The variation of the driving velocity yields variable results because of the relaxation length of the tire, as previously shown in Figure 6-9. Conducting experiments with higher initial velocities yields that $ACL_{50\,\%}$ and ACL_{gain} decrease asymptotical with increasing driving velocity (and, therewith, increasing tire relaxation length), Figure 6-10. The detailed results can be found in annexe B.3.

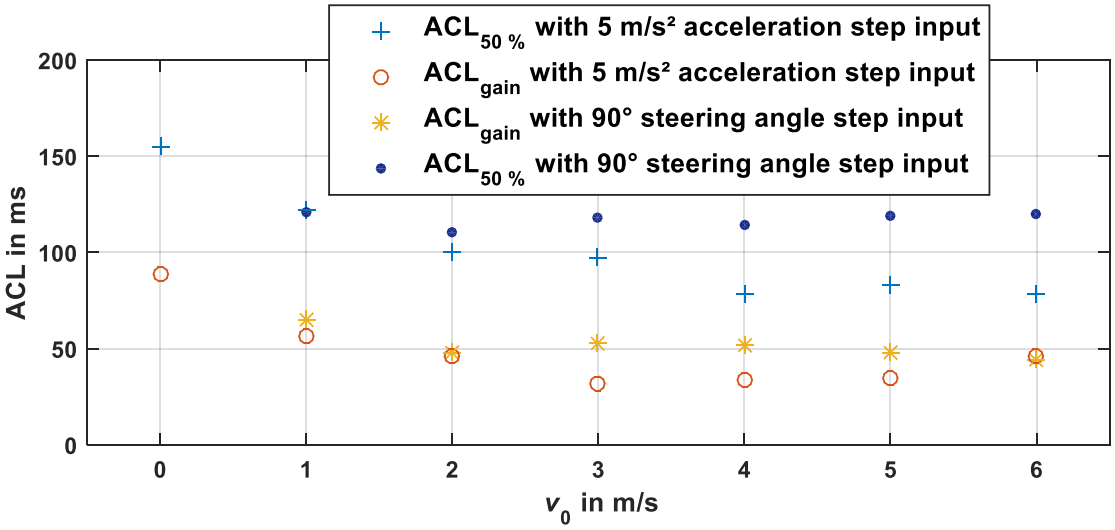

Figure 6-10: $ACL_{50\,\%}$ and ACL_{gain} caused by a constant acceleration or 90° steering angle step input with varied initial velocities (values are averaged over six trials)

The maximum ACL in the constant acceleration step input experiments are found at standstill and are 155 ms for $ACL_{50\,\%}$ and 89 ms for ACL_{gain}, respectively. Additionally, a 90° steering angle step input is investigated, wherein the maximum latencies are 65 ms and 121 ms for ACL_{gain} and $ACL_{50\,\%}$, respectively, and are found at 1 m/s. Noticeable is that the $ACL_{50\,\%}$ for the steering angle step input and the ACL_{gain} for the acceleration step input do not decrease above initial velocities of about 2-3 m/s. For the earlier, this behaviour can be explained by the way the $ACL_{50\,\%}$ is calculated: Because no target acceleration is set, 50 % of the maximum measured acceleration are used as $IACL_{50\,\%}$, thus, resulting in higher values for $ACL_{50\,\%}$ at higher velocities. For the latter, it is not entirely clear why this deviation from the expected behaviour arises. Possible reasons are measurement inaccuracies, too few repetitions, a change in tire temperature (these were the last experiments to be driven), the sensitivity of the $IACL_{gain}$, or a combination of any of these reasons. Because the resulting ACL is far below the requirements, the cause is not further investigated.

6.4.3 Discussion

Two influencing factors (initial velocity, acceleration step input amplitude) and two control input methods (acceleration step input, steering angle step input) were researched. It was shown that the acceleration step input amplitude only affects $ACL_{50\,\%}$, which is because $IACL_{50\,\%}$ is proportional to the acceleration step input amplitude. ACL_{gain} showed no sensitivity on the acceleration step input (Figure 6-9). Therefore, latency itself is not dependent on the acceleration step input amplitude. The initial velocity, however, does have a **major influence: Increasing the driving velocity decreases ACL** because of the tires' relaxation length. This effect is very distinctive at low speeds (Figure 6-9 and Figure 6-10). The differences between the acceleration and steering angle step input are marginal (Figure 6-10), so that the **control method seems to have no significant influence** on the acceleration cue latency.

The $IACL_{50\,\%}$ proved to yield very reproducible values for $ACL_{50\,\%}$, whereas the $IACL_{gain}$ yielded less reproducible results. This is partly caused by the resolution of 2 ms of the time signal, but also by signal disturbance, whose influence is greater on signals with low amplitudes ($IACL_{gain} < IACL_{50\,\%}$ for target amplitudes above 0.4 m/s²). **The requirements** of staying below 135 ms for $ACL_{50\,\%}$ and 100 ms for ACL_{gain}, respectively, **are not met** ($ACL_{50\,\%,max}$ = 159 ms, $ACL_{gain,max}$ = 104 ms). However, for driving velocities of 1 m/s and higher, $ACL_{50\,\%,max}$ is 139 ms and $ACL_{gain,max}$ is 66 ms. Furthermore, the requirement for $ACL_{50\,\%}$ is set by an electric car with a controller that is optimized for instantaneous acceleration. Standard electric cars (e.g. Tesla Model S) need about 250 ms for providing 50 % of the target acceleration.

No direct assessment can be derived for the full-scale WMDS. However, if the novel control approach of keeping the WMDS in motion is implemented and if the steering power is increased appropriately (considering moment of inertia, wheel load, tire width, and tire-road-friction coefficient), the latency requirements can be fulfilled by state-of-the-art technology for full-scale WMDS, too.

Concluding, the aspect of *motion cue latency cannot falsify* hypothesis H1.1, considering the average relative MSD of 14.6 % for ACL_{gain} measurements, the restrictive requirement for $ACL_{50\,\%}$, and the control approach to keep the simulator in motion at any time so that the driving velocity will never become 0.

7 Safety Architecture

A safety architecture is defined as a "set of elements and their interaction to fulfil the safety requirements"[162]. These safety requirements (also called safety goals) have been established for the WMDS prototype MORPHEUS and its unique design. The results of the following risk assessment cannot directly be transferred onto any DS or even the full-scale WMDS. Nevertheless, the risk is assessed for a specific system topology whereas the components are generic. Thus, the assessment is independent of specific components and the established safety requirements are valid for the specified architecture and therewith all instances derived from this architecture. For architectural design changes, methods for adapting an existing risk assessment exist. The specific results for MORPHEUS will be adapted towards a more general application of a full-scale WMDS in section 7.4.

Of course, the quality of the risk analysis and evaluation strongly depends on the expertise of the engineer conducting the analysis. The herein presented risk assessment (sections 7.1 and 7.2) has been carried out by the author who designed, built, and conducted numerous experiments with MORPHEUS and been separately and thoroughly reviewed by an engineer who is familiar with the system but no expert for WMDS as well as by a team of two expert engineers who were involved in the development of MORPHEUS and are also experienced in operating the prototype. Still, this cannot guarantee 100 % safety, which is why a transparent and exhaustive documentation of the HARA is attached in annexe B. Thus, false assumptions or missing failures, consequences, or situations can easily be amended while still being able to keep most of the HARA.

Section 7.1 shows the results of the risk analysis, namely the hazard identification (section 7.1.2) and the risk estimation (section 7.1.3). Together with section 7.2, risk evaluation, the risk assessment process according to EN ISO 13849 (Figure 2-17) is completed. A proposed safety architecture for fulfilling the formulated safety requirements is given in section 7.3 together with an exemplary application of the architecture and an evaluation of achieved risk reduction as well as a risk assessment of the newly introduced components and functions.

[162] ISO TC 22/SC 32 Electrical and electronic components and general system aspects: ISO 26262 (2011). p. 14.

7.1 Risk Analysis

7.1.1 Determination of the Limits of Machinery

The system under investigation is the WMDS **prototype MORPHEUS** (Figure 3-4), fully equipped for driving simulation with a test person. The risk will not be assessed for the entire lifecycle of the system but is focussed on the **operation and maintenance** of the system. Further investigations would be needed for the production and disposal phase of the lifecycle. The energy supply is **entirely electric** (hazardous element).

7.1.1.1 Users

Humans that are possibly interacting with the system are (target and threat):

- System engineer(s) (trained in the interaction with HV systems)
- Mechanic(s)/Maintenance personnel (trained in the interaction with HV systems)
- System operator(s) (trained in the interaction with HV systems)
- Test person
- Uninvolved persons (e.g. bystanders)
- Emergency personnel

7.1.1.2 Use Cases

- Driving Simulation (indirectly controlled by test person inside the WMDS and directly controlled by system operator outside the WMDS)
- Maintenance (e.g. replacing the accumulator)
- Test drives (e.g. with a new MCA setup)
- Transportation (self-propelled or externally propelled)
- Storage
- Emergency rescue (e.g. test person from the WMDS' dome)

7.1.1.3 Components/Subsystems/Structure

The architecture of the prototype itself is structured into seven E/E/PE **subsystems**, whereas all subsystems are mounted to MORPHEUS' structure, except for the external command device that is used stationary and close to MORPHEUS' driving area:

1. Steering units (cf. section 3.2.1)
2. Drive units (cf. section 3.2.1)
3. Hexapod (cf. section 3.2.2)
4. Mock-up (cf. section 3.2.2)
5. External command device
6. WMDS dynamics control (cf. sections 3.3 to 3.5 and section 5.3)
7. Power supply (cf. section 3.2.2)

In the following, these seven subsystems' components, the power and data signal flow within each subsystem and between the subsystems as well as interacting users are described for the chosen architecture. Furthermore, the specific implementation (components, power and data signal flow) in MORPHEUS is shown. A list of all built-in components of MORPHEUS can be found in annexe C.1.

Each **steering and drive unit E/E/PE subsystem** consists of an electric motor (actuator), a motor controller (electronic control unit), and sensors for motor speed (i.e. resolver) and temperature. Additionally, the motor controller has a built-in temperature sensor, a built-in current sensor, and built-in voltage sensors for the input high-voltage supply, the input auxiliary-voltage supply, and the output (high-) voltage supply. All sensor signals are processed in the motor controllers. Each motor controller itself communicates with the central control unit (electronic control unit), from where the controllers get their target values. Thus, the steering and drive units do not communicate directly with each other but only through the central control unit. Because the motor controllers and their programming software are purchased, the safety analysis does not cover the motor controller as an E/E/PE system itself, but rather as a black box reacting to inputs. The energy for the motor controllers is supplied by the LV and HV accumulators of the power supply E/E/PE subsystem. When braking, energy is recuperated from the electric motors, forwarded to the motor controllers, and sent back to the HV accumulator. The steering and drive unit E/E/PE subsystems are only directly interacted with by the maintenance personnel and/or system engineer(s).

Figure 7-1 gives an overview of the components that are included in MORPHEUS' steering and drive unit E/E/PE subsystems, whereas the italic labels represent sensors and arrows indicate the direction of flow of power and information signals:

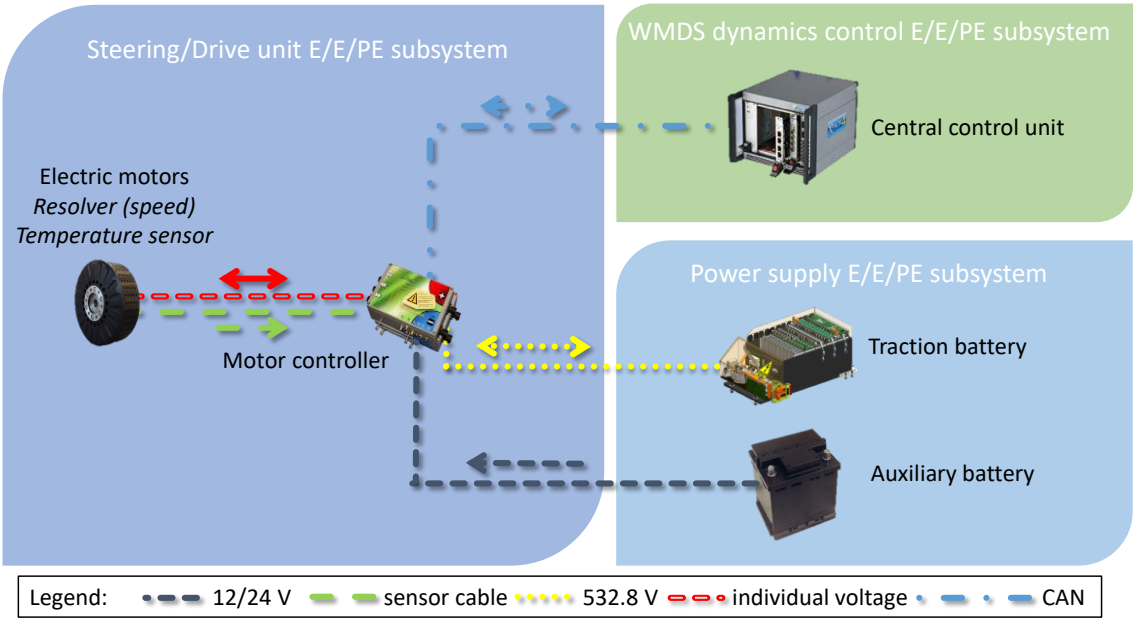

Figure 7-1: MORPHEUS' steering/drive unit E/E/PE subsystem

The **hexapod E/E/PE subsystem** consists of six electric linear actuators, a power electronics unit, and sensors for the actuators' position and temperature. The sensor setup of the power electronics is not known. The power electronics sends and receives data to/from the central control unit. In contrast to the steering and drive units, the power electronics unit communicates with all six linear actuators. Because the power electronics unit is purchased, the safety analysis does not cover the power electronics as an E/E/PE system itself, but rather as a black box reacting to inputs. The energy for the power electronics is supplied by the HV accumulator of the power supply E/E/PE subsystem. The hexapod E/E/PE subsystem is only directly interacted with by the maintenance personnel and/or system engineer(s).

Figure 7-2 gives an overview of the components that are included in the MORPHEUS' hexapod E/E/PE subsystem, whereas the italic labels represent sensors and arrows indicate the direction of flow of power and information signals:

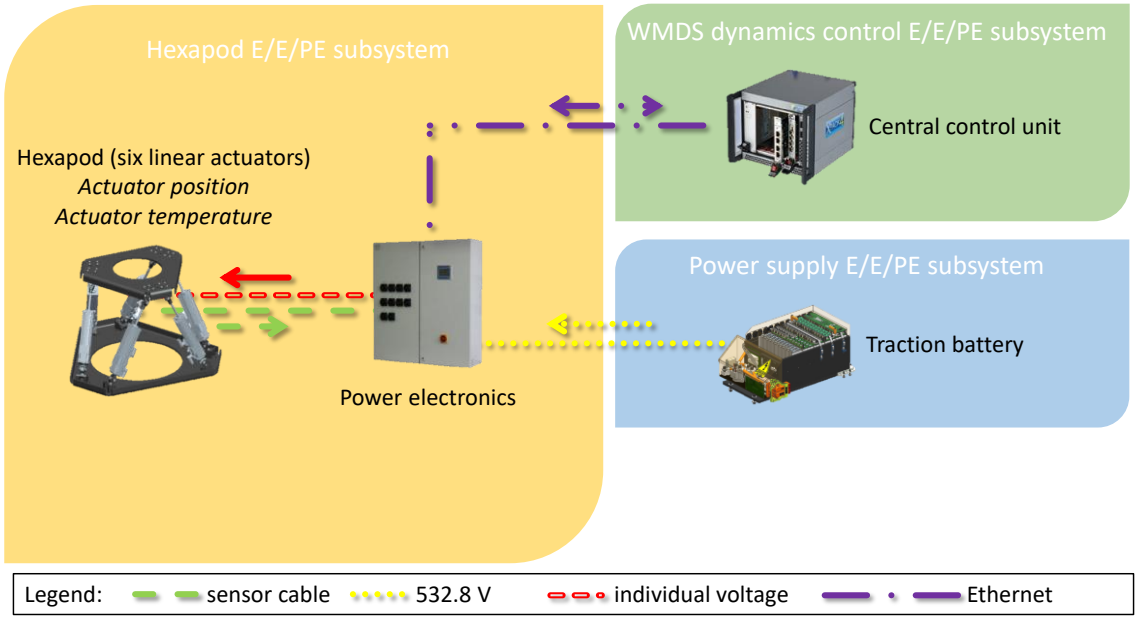

Figure 7-2: MORPHEUS' hexapod E/E/PE subsystem

The **mock-up E/E/PE subsystem** senses gear selection, steering wheel angle, and clutch, brake, and accelerator pedal position, which are commanded by the test person (sensors). Active steering wheel force feedback and an ABS shaker (actuators) provide tactile feedback to the driver. A vision system (e.g. screens, projectors, or a head-mounted display) and a sound system provide visual and audible feedback to the driver. A communication system allows bidirectional oral communication with the system operator. A surveillance system monitors the test person (e.g. seating position, health, safety belt, etc.). An air conditioning system provides a pleasant climate for the test person. The system operator sets the target values for air temperature and humidity manually. All information gathered in the mock-up itself is forwarded to the central control unit (electronic control unit). The communication and surveillance system, on the other hand, communicates directly with the communication and surveillance system of the external command device E/E/PE subsystem through a wireless protocol. The power is supplied by an AC/DC converter of the power supply E/E/PE subsystem. The mock-up E/E/PE subsystem is directly interacted with by the test person, maintenance personnel, system engineer(s), and eventually emergency personnel.

Figure 7-3 gives an overview of the components that are included in MORPHEUS' mock-up E/E/PE subsystem, whereas the italic labels represent sensors/interfaces and arrows indicate the direction of flow of power and information signals:

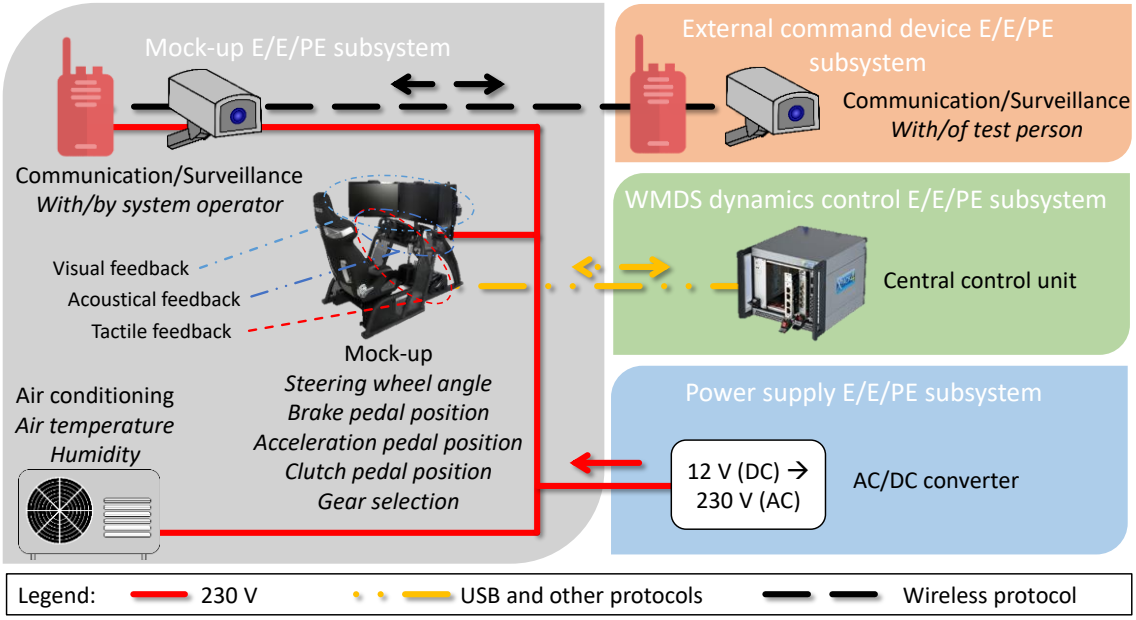

Figure 7-3: MORPHEUS' mock-up E/E/PE subsystem

The **external command device E/E/PE subsystem** is the HMI between system operator(s) and WMDS. The HMI senses the operator's inputs and forwards the input signals to the central control unit. With the HMI, the operator can start and stop simulation runs, change simulation parameters, and control specific functions of the WMDS (e.g. manual drive). Also, he can communicate orally and bidirectional with the test person. Relevant information about the WMDS' state is retrieved from the central control unit through a wireless protocol and shown on the HMI. The communication and surveillance system, on the other hand, communicates directly and wirelessly with the communication and surveillance system in the mock-up E/E/PE subsystem. The power is supplied by a stationary power supply (i.e. power socket) of the power supply E/E/PE subsystem. The system operator(s), maintenance personnel, system engineer(s), and possibly mechanic(s) interact directly with the external command device E/E/PE subsystem.

Figure 7-4 gives an overview of the components that are included in MORPHEUS' external command device E/E/PE subsystem, whereas the italic labels represent inputs/interfaces and arrows indicate the direction of flow of power and information signals:

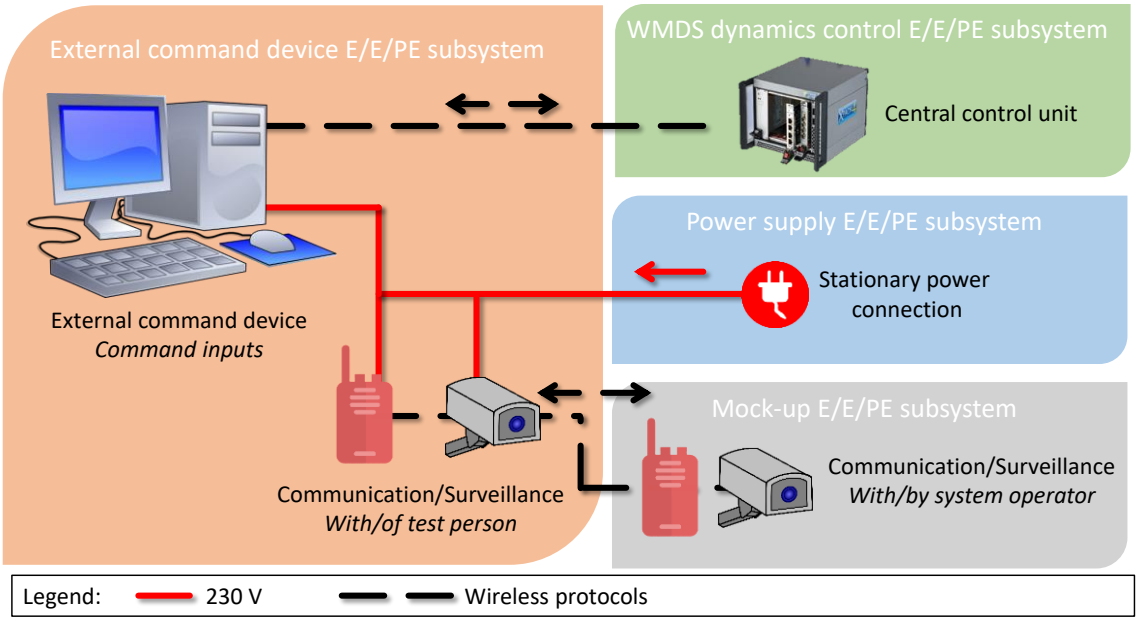

Figure 7-4: MORPHEUS' external command device E/E/PE subsystem

The **WMDS dynamics control E/E/PE subsystem** consists of the central control unit (electronic control unit) and a measurement unit for motion quantities (sensors, namely translational and rotational acceleration and velocity as well as the absolute position within a reference COS). These signals are gathered together with the sensor signals from the steering and drive units, the hexapod, and the mock-up in the central control unit to calculate the overall WMDS state. From here, the vehicle simulation, the MCA, and the MC are executed and target values for the subsystems 1-4 are calculated. The communication with the external command device E/E/PE subsystem is wireless. Power is supplied by the auxiliary battery of the power supply E/E/PE subsystem. The WMDS dynamics control E/E/PE subsystem is only directly interacted with by the system engineer(s) and possibly mechanic(s).

Figure 7-5 gives an overview of the components that are included in MORPHEUS' dynamic control E/E/PE subsystem, whereas the italic labels represent sensors and arrows indicate the direction of flow of power and information signals:

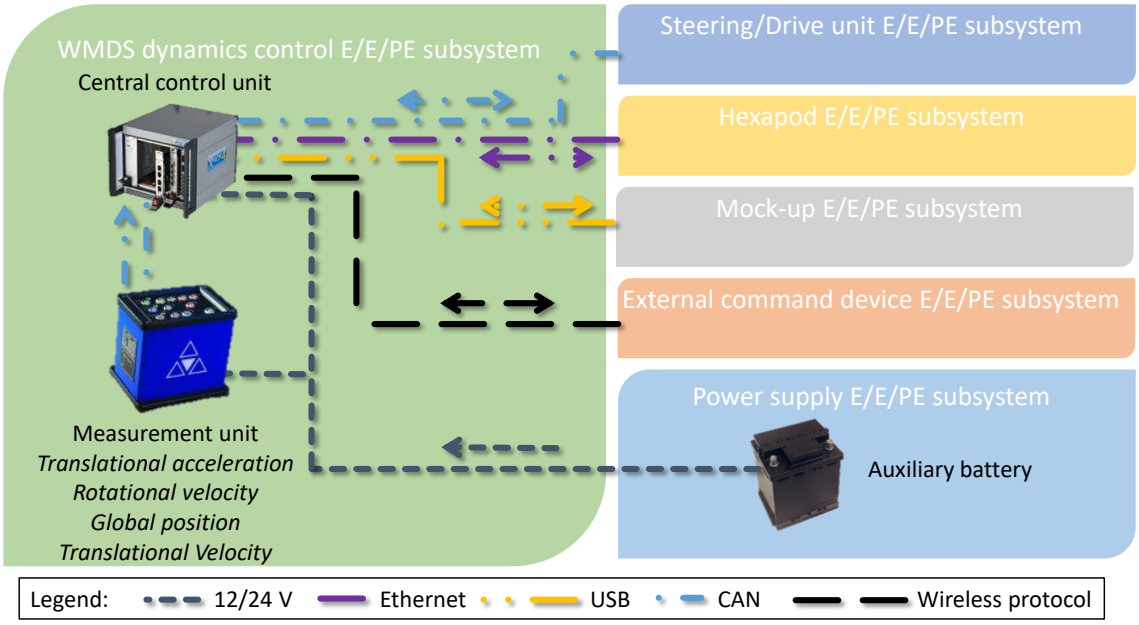

Figure 7-5: MORPHEUS' dynamics control subsystem

The **power supply E/E/PE subsystem** consists of a traction battery (HV), an auxiliary battery (LV), a stationary power connector (power socket), and an AC/DC converter (all hazardous elements). The converter transforms the direct current of the auxiliary battery to alternating current. The auxiliary BMS (electronic control unit) monitors its voltage (sensor). The traction BMS (electronic control unit) monitors its temperature, voltage, and current (sensors) and can operate its power contactors (actuator). If the temperature is in a critical range or if the voltage or current are above a certain threshold, the traction battery's power supply is cut. LV power is provided to the steering unit, drive unit, and WMDS dynamics control E/E/PE subsystems; HV power to the steering unit, drive unit, and hexapod E/E/PE subsystems. Alternating current is provided to the mock-up (from AC/DC converter) and the external command device (from stationary power connector) E/E/PE subsystems. The state of charge (SOC) of the traction and auxiliary battery is forwarded to the central control unit. Because the auxiliary and traction batteries and their BMS are purchased, the safety analysis does not cover the batteries as an E/E/PE system themselves, but rather as black boxes reacting to inputs. The power supply E/E/PE subsystem is only directly interacted with by the system engineer(s) and possibly mechanic(s) and/or the system operator(s).

Figure 7-6 gives an overview of the components that are included in MORPHEUS' power supply E/E/PE subsystem, whereas the italic labels represent signals and arrows indicate the direction of flow of power and information signals:

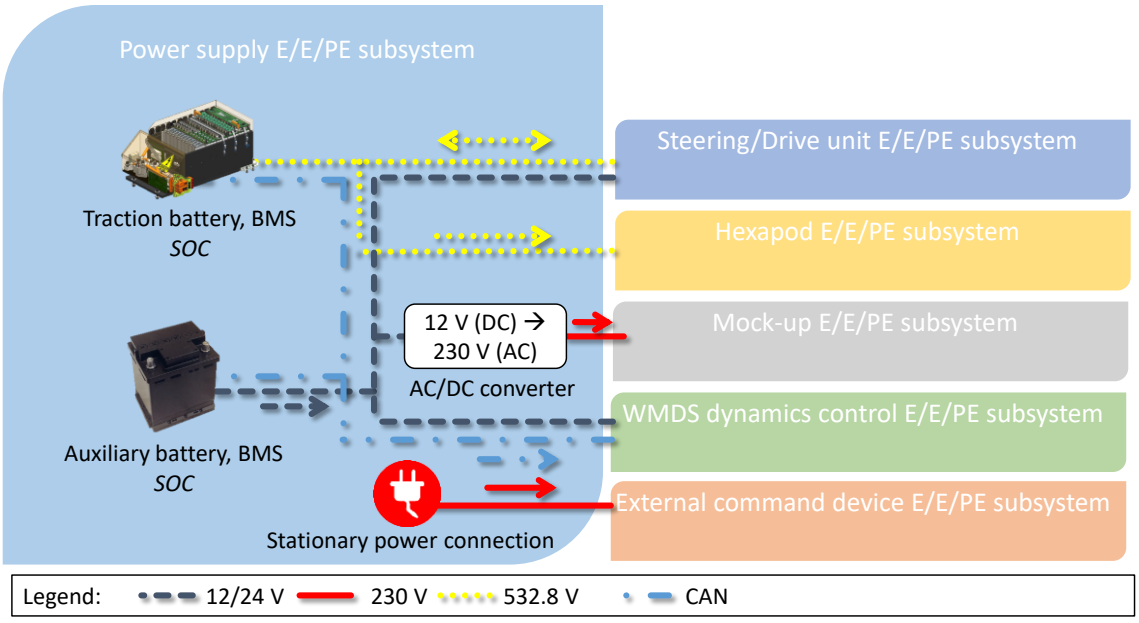

Figure 7-6: MORPHEUS' power supply E/E/PE subsystem

7.1.1.4 Environment

The controlled **environment**, in which the system will be used, can be inside (e.g. a hall) or outside (e.g. a vehicle dynamics test area) and includes the following conditions:

- Air temperature: -10 °C to +45 °C
- Humidity: 0 % to 85 % (condensation must be avoided)
- Direct solar radiation
- Paved undergrounds with no obstacles (objects and subjects; WMDS workspace must be inspected before the DS may move; boundaries of the workspace must be highlighted and monitored or cordoned off so that subjects cannot enter the workspace) and sufficient tire-underground friction coefficient (i.e. no ice or snow)
- No rain or fog
- Low level of pollution (for E/E/PE components)
- Wind up to level 6 on the Beaufort scale (i.e. strong breeze with wind speeds up to 49 km/h, description: "Large branches in motion; whistling heard in telegraph wires; umbrellas used with difficulty") resulting – at -10 °C air temperature – in a wind chill temperature[163] of -21.7 °C.

7.1.2 Hazard Identification

The methodology for the hazard identification is described in section 4.4.2. Each subsystem's components and their interconnections are investigated and – in combination with the guidewords from the HAZOP analysis – evaluated, which failures might occur. Because the extent of the hazard list is too large to be shown within this thesis, the complete list is attached in annexe C.2 (columns "failure" and "consequence"). At this point, three examples are selected to demonstrate the application of the methodology.

7.1.2.1 Hazard 1.2 (Steering Unit E/E/PE Subsystem)

Failure: No or insufficient LV energy supply

Consequence: The motor controller is unable to process its signals → demanded steering angle cannot be provided → DS trajectory is uncontrollable

The LV energy supply is only connected to the motor controller in a steering unit E/E/PE subsystem. If the voltage supplied by the LV energy supply is insufficient, the motor controller automatically shuts itself down. Thus, the target values from the WMDS driving dynamics control subsystem cannot be processed by the motor controller. The electric steering motor cannot be controlled by the motor controller and the demanded DS trajectory cannot be realized because the required steering angles cannot be adjusted.

[163] Osczevski, R.; Bluestein, M.: Wind Chill Equivalent Temperature Chart (2005).

7.1.2.2 Hazard 2.8 (Drive Unit E/E/PE Subsystem)

Failure: Temperature sensor delivers no/too low/high electric motor temperature signals

Consequence 1: Motor controller reduces maximum electric motor torque or shuts electric motor down → demanded motor torque cannot be provided → DS trajectory is not controllable

Consequence 2: Motor controller fails to reduce electric motor torque or to shut electric motor down → overheating of electric motor → possibly short circuit and/or fire hazard

Here, two consequences are possible. One consequence is that, although the electric motor is operated within its specifications, the temperature sensors may send a signal to the motor controller that the electric motor is too cold, too hot, or sends no signal at all. In all these cases the motor controller would either reduce the maximum electric motor torque or shut down the electric motor completely. A possible outcome would be that the demanded motor torque cannot be provided due to the derating or shutdown of the drive motor.

The other possible consequence is that the electric motor is outside its specified temperature range, although the temperature sensor sends an uncritical signal. Then, the motor controller would not reduce the maximum electric motor torque or shut the motor down. This could cause the electric motor to overheat, possibly resulting in a short circuit or a fire hazard.

7.1.2.3 Hazard 4.20 (Mock-up E/E/PE Subsystem)

Failure: Water ingress at steering wheel

Consequence 1: Short circuit and possibly fire hazard

Consequence 2: Steering wheel force feedback actuator is unable to operate → false cues are generated

Consequence 3: Steering wheel angle sensor is unable to operate → false cues are generated

The first consequence of water ingress at the steering wheel could be a short circuit and possibly a fire hazard.

The second consequence is a possible malfunction of the steering wheel force feedback actuator. Then, the test person would not get tactile feedback about the virtual car's driving state, resulting in a degenerated immersion.

The third potential consequence is a malfunction of the steering wheel angle sensor. In this case, the test person's steering angle input could not be sensed. The virtual car and, thus, the DS would not follow the desired trajectory, resulting in false cues. This hazard

is not critical in terms of the WMDS' trajectory, because the trajectory of the virtual car is not directly linked to the trajectory of the WMDS that is calculated by the WMDS dynamics control subsystem. Thus, collisions are avoided independently of the test person's input.

7.1.3 Risk Estimation

The identified hazards are investigated in each use case, with each user and in each environmental condition to find the most critical combination. This combination results in a description of the worst-case situation, in which the hazard occurs. The elements failure, consequence, and situation describe the full hazardous event, whose risk is now to be evaluated. Therefore, the risk parameters C, F, P, and W (see Table 2.4, section 2.3.2) are estimated according to IEC 61508 and the hazardous event's risk is determined with the risk graph method (see Figure 2-16, section 2.3.2). The full list of 186 evaluated combinations of failures, consequences, and situations can be found in annexe C.2. For demonstrating the application of the prescribed methodology, the risk for the same three examples as described in the previous section is estimated:

7.1.3.1 Hazardous Event 1.2 (Steering Unit E/E/PE Subsystem)

Failure: No or insufficient LV energy supply

Consequence: DS trajectory is uncontrollable

Situation: Driving simulation with test person, high velocity, close to boundary of DS workspace

The worst situation, in which hazard 1.2 could occur, is the driving simulation use case with a test person, whereas the WMDS moves with high (close to maximum) velocity and close to the boundary of the DS workspace. If the hazard occurs and the WMDS' trajectory is uncontrollable, the WMDS might crash into objects and/or subjects outside its workspace boundaries. The risk for this hazardous event is estimated as follows:

Consequence: C3 (Death to several people)

The test person and/or bystanders and/or the system operator(s) may be injured and/or killed.

Frequency: F2 (Frequent to permanent exposure in the hazardous zone)

The driving simulation use case is the standard application for the EUC and is very frequently used. Also, the boundaries of the workspace are reached often, and high velocities are driven.

Poss. of avoid.: P2 (Almost impossible)

Although the system operator is skilled, a LV power cut occurs very suddenly and can hardly be foreseen prior to the hazardous event. Once the hazard has occurred, the system operator has no possibility of mitigating the event, because he cannot steer the WMDS anymore.

Probability: W1 (A very slight probability that the unwanted occurrences will come to pass, and only a few unwanted occurrences likely)

Standard LV accumulators and a standard BMS are used, which makes a LV power cut more unlikely than a HV power cut, where a prototype HV accumulator is used in combination with a safety-orientated BMS.

The combination of the risk parameters results in a SIL of *2* for hazardous event 1.2.

7.1.3.2 Hazardous Event 2.8 (Drive Unit E/E/PE Subsystem)

Failure: Temperature sensor delivers no/too low/high electric motor temperature signals

Consequence 1: DS trajectory is uncontrollable

Situation 1: Driving simulation with test person, high velocity, close to boundary of DS workspace

For consequence 1, the same situation is used as in hazardous event 1.2: Driving simulation with a test person, whereas the WMDS moves with high (close to maximum) velocity and close to the boundary of the DS workspace. The risk for this hazardous event is estimated as follows:

Consequence: C3 (Death to several people)

The test person and/or bystanders and/or the system operator(s) may be injured and/or killed.

Frequency: F2 (Frequent to permanent exposure in the hazardous zone)

The driving simulation use case is the standard application for the EUC and is very frequently used. Also, the boundaries of the workspace are reached often, and high velocities are driven.

Poss. of avoid.: P1 (Possible under certain conditions)

The skilled system operator can observe the temperature and, therefore, detect a faulty temperature signal. Furthermore, if only one temperature sensor and, therewith, electric motors fails, acceleration/deceleration is still possible to some extent with the other two electric motors. Steering and mitigation are possible as well.

Probability: W1 (A very slight probability that the unwanted occurrences will come to pass, and only a few unwanted occurrences likely)

The supplier developed its electric motor (and temperature sensor) according to applicable standards. The motor is also used in light aircrafts.

The combination of the risk parameters results in a SIL of *1* for hazardous event 2.8.1.

Consequence 2: Short circuit and/or fire hazard

Situation 2: Driving simulation with test person, test person must be rescued from dome

For consequence 2, another situation is identified: A high risk exists with the driving simulation use case with an unskilled test person in case of short circuit and/or fire. The test person will get injured and so may be the emergency personnel that is trying to rescue the test person. The risk for this hazardous event is estimated as follows:

Consequence: C3 (Death to several people)

The test person and/or the emergency personnel may be seriously injured or killed by either short circuit or fire.

Frequency: F2 (Frequent to permanent exposure in the hazardous zone)

The driving simulation use case is the standard application for the EUC and is very frequently used.

Poss. of avoid.: P1 (Possible under certain conditions)

The skilled system operator can observe the temperature and therefore detect a faulty temperature signal. Mitigation is possible.

Probability: W1 (A very slight probability that the unwanted occurrences will come to pass, and only a few unwanted occurrences likely)

The suppliers developed their electric motor (and temperature sensor) and motor controller according to applicable standards. The motor is also used in light aircrafts.

The combination of the risk parameters results in a SIL of *1* for hazardous event 2.8.2.

7.1.3.3 Hazardous Event 4.20 (Mock-up E/E/PE Subsystem)

Failure: Water ingress at steering wheel

Consequence 1: Short circuit and possibly fire hazard

Situation 1: Driving simulation with test person, test person must be rescued from dome

For consequence 1, the worst situation is any driving simulation use case with a test person. The test person will get injured and so may be the emergency personnel that is trying to rescue the test person. The risk for this hazardous event is estimated as follows:

Consequence: C3 (Death to several people)

The test person and/or the emergency personnel may be seriously injured or killed either by short circuit or fire.

Frequency: F2 (Frequent to permanent exposure in the hazardous zone)

The driving simulation use case is the standard application for the EUC and is very frequently used.

Poss. of avoid.: P1 (Possible under certain conditions)

The skilled system operator can take countermeasures if rain/snow etc. arises so that no water ingress can be caused by weather. Mitigation is possible.

Probability: W2 (A slight probability that the unwanted occurrences will come to pass, and few unwanted occurrences are likely)

The previously determined limits of the machinery exclude wet and moist environmental conditions. Still, users interacting with the system could bring liquid, e.g. for drinking.

The combination of the risk parameters results in a SIL of *2* for hazardous event 4.20.1.

Consequence 2: False cues are generated

Consequence 3: False cues are generated

Situation 2/3: Driving simulation with test person, dynamic driving situation

For consequence 2 and 3, the worst situation is the driving simulation use case with a test person, whereas the WMDS moves with high amplitude and frequency accelerations. The risk for this hazardous event is estimated as follows:

Consequence: C1 (Minor injury)

Because of the representation of false cues in a highly dynamic driving situation, motion sickness may occur.

Frequency: F2 (Frequent to permanent exposure in the hazardous zone)

The driving simulation use case is the standard application for the EUC and is very frequently used. Also, highly dynamic driving situations are very frequently simulated.

Poss. of avoid.: P1 (Possible under certain conditions)

The skilled system operator can take countermeasures if rain/snow etc. arises so that no water ingress can be caused by weather. Mitigation is possible.

Probability: W2 (A slight probability that the unwanted occurrences will come to pass, and few unwanted occurrences are likely)

The previously determined limits of the machinery exclude wet and moist environmental conditions. Still, users interacting with the system could bring liquid, e.g. for drinking.

The combination of the risk parameters results in a SIL of *a* for the hazardous events 4.20.2 and 4.20.3.

7.2 Risk Evaluation

From the hazard list, safety requirements are established, whereas each safety function requirement is assigned to a safety integrity requirement (i.e. SIL). Safety function requirements with a safety integrity requirement of level *a* are rather requirements for quality management than functional safety. It is important to understand that some safety functions requirements cannot be fulfilled to the full extent in which they are formulated because there is no 100 % guarantee that a failure will not occur. Here, the safety integrity requirement defines the likelihood with which a failure is allowed to occur. Sections 7.2.1 to 7.2.5 present the safety function requirements, classified by their highest corresponding safety integrity requirement. The underlying hazardous event as well as the risk classification is pointed out for every safety function requirement, denoted after each requirement with the nomenclature (No. of hazardous event; C level, F level, P level, W level). Concluding, a summary of the required safety functions is given in section 7.2.6.

7.2.1 SIL *4* Safety Function Requirements

- The **DS trajectory must remain controllable** (so that collisions with objects and subjects can be avoided) in case of
    - a faulty data transmission from the central control unit to the drive unit subsystem (No. 6.9; C3, F2, P2, W3)

7.2.2 SIL *3* Safety Function Requirements

- The DS trajectory must remain controllable (so that collisions with objects and subjects can be avoided) in case of
    - a faulty data transmission from
        - the central control unit to the external command device subsystem (No. 6.12; C3, F1, P2, W3)
        - the central control unit to the hexapod subsystem (No. 6.10; C3, F1, P2, W3)

        - the central control unit to the steering unit subsystem (No. 6.8; C3, F1, P2, W3)
    - an HV power cut (No. 7.1; C3, F2, P2, W2)
    - an overvoltage from the steering/drive unit subsystem (during recuperation) (No. 7.6.1; C3, F2, P1, W3)
- **Continuous short circuit must be avoided** so that during a rescue other subjects cannot get an electric shock (No. 7.6.2; C3, F2, P1, W3)
- **HV overvoltage** (because of recuperation) **must be avoided** (No. 7.6.2; C3, F2, P1, W3)

7.2.3 SIL *2* Safety Function Requirements

- The DS trajectory must remain controllable (so that collisions with objects and subjects can be avoided) in case of
    - a faulty auxiliary battery's SOC signal to the WMDS dynamics control system (No. 7.15; C3, F2, P2, W1)
    - a faulty traction battery's SOC signal to the WMDS dynamics control system (No. 7.14; C3, F2, P2, W1)
    - a faulty data transmission from
        - the external command device to the WMDS dynamics control subsystem (No. 5.5; C3, F1, P2, W2)
        - the central control unit to the mock-up subsystem (No. 6.11; C1, F2, P2, W3)
        - a motor controller to the central control unit (No. 1.14 & 2.14; C3, F2, P2, W1)
    - an HV overvoltage (No. 1.3.1 & 2.3.1; C3, F2, P1, W2; No. 7.2.1; C3, F2, P2, W1)
    - an LV power cut (No. 6.1; C3, F2, P2, W1)
    - an AC/DC converter overvoltage (No. 7.4.1; C3, F2, P2, W1)
    - a faulty measurement from the measurement unit for motion quantities (No. 6.13; C3, F2, P1, W2)
    - water ingress at
        - the measurement unit for motion quantities (No. 6.4.2; C3, F2, P1, W2)
        - an electric motor (No. 1.12.3 & 2.12.3; C3, F2, P1, W2)
        - the central control unit (No. 6.3.2; C3, F2, P1, W2)
        - a motor controller (No. 1.13.3 & 2.13.3; C3, F2, P1, W2)
        - the AC/DC converter (No. 7.9.1; C3, F2, P1, W2)
        - an auxiliary battery (No. 7.8.1; C3, F2, P1, W2)
        - the traction battery (No. 7.7.1; C3, F2, P1, W2)

- **AC/DC converter overvoltage must be avoided (**No. 7.4.1 & 7.4.2; C3, F2, P2, W1)
- **Auxiliary battery's temperature must be monitored** (No. 7.12; C3, F2, P2, W1)
- **Water ingress** at the following components **must be avoided**
  - AC/DC converter (No. 7.9.1 & 7.9.2; C3, F2, P1, W2)
  - auxiliary battery (No. 7.8.1 & 7.8.2; C3, F2, P1, W2)
  - electric motor (No. 1.12.1, 1.12.3, 2.12.1 & 2.12.3; C3, F2, P1, W2)
  - motor controller (No. 1.13.1, 1.13.3, 2.13.1 & 2.13.3; C3, F2, P1, W2)
  - hexapod actuator (No. 3.11.1; C3, F2, P1, W2)
  - hexapod power electronics (No. 3.12.1; C3, F2, P1, W2)
  - stationary power connector (No. 7.10.2; C3, F2, P1, W2)
  - measurement unit for motion quantities (No. 6.4.1 & 6.4.2; C3, F2, P1, W2)
  - external command device (No. 5.3.1; C3, F2, P1, W2)
  - central control unit (No. 6.3.1 & 6.3.2; C3, F2, P1, W2)
  - pedals (No. 4.21.1, 4.22.1, 4.23.1 & 4.24.1; C3, F2, P1, W2)
  - sound system (No. 4.19.1; C3, F2, P1, W2)
  - steering wheel (No. 4.20.1; C3, F2, P1, W2)
  - visual representation system (No. 4.18.1; C3, F2, P1, W2)
  - traction battery (No. 7.7.1; C3, F2, P1, W2)
- The **test person must be able to communicate with the system operator and vice versa** in case of
  - a faulty data transmission from the external command device to the WMDS dynamics control subsystem (No. 5.6; C2, F2, P2, W2)
- **The wireless data transmission must not fail** (No. 5.6; C2, F2, P2, W2)

7.2.4 SIL *1* Safety Function Requirements

- The DS trajectory must remain controllable (so that collisions with objects and subjects can be avoided) in case of
  - a faulty data transmission from the measurement unit for motion quantities to the central control unit (No. 6.7; C3, F2, P1, W1)
  - an LV overvoltage (No. 1.4.1, 2.4.1, 6.2.1, 6.2.2 & 7.3.1; C3, F2, P1, W1)
  - a stationary power cut (No. 5.1.1 & 5.1.2; C3, F1, P2, W1)
  - water ingress at the
    - external command device (No. 5.3.2; C3, F1, P1, W2)
    - stationary power connector (No. 7.10.1; C3, F2, P1, W1)
  - a malfunctioning
    - measurement unit for motion quantities (No. 6.6.1; C3, F2, P1, W1)

        - central control unit (No. 6.5.1; C3, F2, P1, W1)
        - AC/DC converter (No. 7.13.1; C3, F2, P1, W1)
        - electric motor (No. 1.5.1, 1.6, 1.7, 1.8.1, 1.10.1, 2.5.1, 2.6, 2.7, 2.8.1 & 2.10.1; C3, F2, P1, W1)
        - motor controller (No. 1.9.1, 1.11.1, 2.9.1 & 2.11.1; C3, F2, P1, W1)
        - traction battery (No. 7.11.1; C3, F2, P1, W1)
- A **stationary power overvoltage must be avoided** (No. 5.2.2; C3, F2, P1, W1)
- Water ingress at the following components must be avoided
    - air conditioning system (No. 4.24.2; C2, F2, P2, W1)
    - communication system (No. 4.22.2; C2, F2, P1, W2)
- **Air conditioning must be available** (No. 4.24.2; C2, F2, P2, W1)
- The test person must be able to communicate with the system operator and vice versa in case of
    - water ingress at the communication system (No. 4.22.2; C2, F2, P1, W2)
- The **test person must remain accessible** in case of
    - a HV power cut (No. 3.1; C2, F1, P2, W2)
- **The service engineer(s) and/or mechanic(s) or test person must not be seriously injured or killed if the dome becomes loose or instable** (No. 3.3.2, 3.5, 3.7.1 & 3.10; C3, F1, P2, W1; No. 3.3.1; C2, F2, P2, W1)

7.2.5 SIL *a* Safety Function Requirements

- The DS trajectory must remain controllable (so that collisions with objects and subjects can be avoided) in case of
    - a malfunctioning external command device (No. 1.5.2; C3, F1, P1, W1)
    - a stationary power connector overvoltage (No. 5.2.1 & 7.5.1; C3, F1, P1, W1)
- Water ingress at the following components must be avoided
    - surveillance system (No. 4.23.2; C2, F1, P1, W2)
- Test person must be able to communicate with the system operator and vice versa in case of
    - an AC/DC converter power cut (No. 4.1.2; C2, F1, P2, W1)
    - an AC/DC converter overvoltage (No. 4.2.3; C2, F1, P1, W1)
    - a malfunctioning communication system (No. 4.15.1, C2, F1, P1, W2)
    - Water ingress at the external command device (No. 5.3.2; C2, F1, P1, W2)
    - a faulty data transmission from the mock-up's communication system to the external command device's communication system (No. 4.25; C2, F1, P1, W2)
    - a stationary power cut (No. 5.1.3; C2, F1, P2, W1)

- The following signals must be correctly sensed
  - Accelerator pedal position (No. 4.2.1, 4.14.1 & 4.21.3; C1, F2, P1, W1; No. 4.1.1; C1, F2, P2, W1)
  - Brake pedal position (No. 4.2.1, 4.6, 4.14.1 & 4.21.3; C1, F2, P1, W1; No. 4.1.1; C1, F2, P2, W1)
  - Clutch pedal position (No. 4.2.1, 4.5, 4.14.1 & 4.21.3; C1, F2, P1, W1; No. 4.1.1; C1, F2, P2, W1)
  - Gear selection (No. 4.2.1, 4.3 & 4.14.1; C1, F2, P1, W1; No. 4.1.1; C1, F2, P2, W1)
  - Steering wheel angle (No. 4.2.1 & 4.4; C1, F2, P2, W1; No. 4.14.1 & 4.20.3; C1, F2, P1, W1; No. 4.1.1; C1, F2, P2, W1)
- The following cues must be correctly provided
  - ABS shaker feedback (No. 4.2.2, 4.9 & 4.13.1; C1, F2, P1, W1; No. 4.21.2; C1, F2, P1, W2; No. 4.1.3; C1, F2, P2, W1; No. 4.1.4; C3, F1, P1, W1)
  - acoustical feedback (No. 4.2.2, 4.10 & 4.13.1; C1, F2, P1, W1; No. 4.19.2; C1, F2, P1, W2; No. 4.1.3; C1, F2, P2, W1; No. 4.1.4; C3, F1, P1, W1)
  - steering wheel force feedback (No. 4.2.2, 4.8 & 4.13.1; C1, F2, P1, W1; No. 4.20.2; C1, F2, P1, W2; No. 4.1.3; C1, F2, P2, W1; No. 4.1.4; C3, F1, P1, W1)
  - visual feedback (No. 4.2.2, 4.11 & 4.13.1; C1, F2, P1, W1; No. 4.18.2; C1, F2, P1, W2; No. 4.1.3; C1, F2, P2, W1; No. 4.1.4; C3, F1, P1, W1)
- Malfunctioning hexapod’s power electronics must be avoided (No. 3.7.2; C1, F2, P2, W1)
- The system operator must be able to monitor the test person (No. 4.1.5 & 4.1.6; C2, F1, P2, W1; No. 4.2.4 & 4.16.1; C2, F1, P1, W1; No. 4.23.2 & 4.26; C2, F1, P1, W2)
- The test person must remain accessible in case of
  - a faulty data transmission from the hexapod’s power electronics to the central control unit (No. 3.13; C2, F1, P2, W1)
  - a malfunctioning hexapod actuator (No. 3.4, 3.6.1, 3.8.1 & 3.9.1; C2, F1, P1, W1; No. 3.11.4; C2, P1, F1, W2)
  - an HV overvoltage (No. 3.2.1; C2, F1, P1, W2)
- The test person's inputs must be correctly forwarded to the central control unit (No. 4.14.1; C1, F2, P1, W1)

7.2.6 Conclusion

SIL *a* safety requirements are not considered in the following. Also, case discriminations are left out so that hazards are addressed in general and the highest demanded safety integrity requirement is assigned to the generalised hazards. Concluding, the following safety functions must be provided:

1. The DS trajectory must remain controllable so that collisions with objects and subjects can be avoided. (SIL *4*)
2. Continuous short circuit must be avoided so that during a rescue other subjects cannot get an electric shock. (SIL *3*)
3. HV overvoltage (because of recuperation) must be avoided. (SIL *3*)
4. AC/DC converter overvoltage must be avoided. (SIL *2*)
5. Auxiliary battery's temperature must be monitored. (SIL *2*)
6. Water ingress at all E/E/PE systems must be avoided. (SIL *2*)
7. The test person must be able to communicate with the system operator and vice versa. (SIL *2*)
8. The wireless data transmission must not fail. (SIL *2*)
9. Stationary power overvoltage must be avoided. (SIL *1*)
10. Air conditioning must be available at all times. (SIL *1*)
11. The test person must remain accessible. (SIL *1*)
12. The service engineer(s) and/or mechanic(s) or test person must not be seriously injured or killed if the dome becomes loose or instable. (SIL *1*)

7.3 Proposed Architectural Design

Because failures cannot be entirely avoided, the risk is reduced by reducing the failure's probability of occurrence or by mitigating the consequence of a hazard. Possible risk reduction measures can be to apply safety-certified technologies, to stipulate conduct guidelines or initialisation processes, to employ redundancies, or to implement external risk reduction facilities. In any case, a revised HARA will be needed to prove the effectiveness of the risk reduction measures and to assess if new risks are generated. Again, the process is iterative. Safety functions influence each other and, therefore, may reduce or increase the safety integrity requirements of other functions. In this section it will be evaluated how the identified safety functions can be provided (section 7.3.1). Concluding, the resulting overall safety architecture is presented (section 7.3.2) and an exemplary safety architecture is designed and assessed in terms of risk (section 7.3.3).

7.3.1 Safety Functions and Proposed Implementation

7.3.1.1 DS Trajectory Must Remain Controllable (SIL *4*)

The most important and critical safety function to be provided is the controllability of MORPHEUS' trajectory. The function is required to be available in case of faulty data transmission between the subsystems, any power cuts or overvoltage, faulty battery SOC signals, incorrect data from the measurement unit for motion quantities, water ingress at any E/E/PE system, or a general malfunction of any E/E/PE system, although with different safety integrity requirements. Clearly, it is hardly possible to avoid all the prescribed failures at the demanded safety integrity levels. Therefore, it is advisable to mitigate the consequences of the manifold failures. Using redundancies for all possible failures would practically result in building two WMDS onto one frame structure and would therefore contradict the lightweight concept. Thus, an external risk reduction facility is favoured, which is a common approach for smallest-scale production series.

The external risk reduction facility is required to control MORPHEUS' trajectory independently of components that could contribute to a hazardous event, namely electric motors, motor controllers, external command device, central control unit, measurement unit for motion quantities, and the entire power supply. Furthermore, the failures leading to hazardous events must be continuously monitored so that the external risk reduction facility is automatically triggered. Possible designs must provide their own energy. The trajectory can be controlled in two ways: Either by using the tire-underground-pairing of the WMDS or by using an independent force transmission system (e.g. friction-based or momentum-based). The design must be able to significantly influence the trajectory while being able to counteract the maximum forces that can be applied by the WMDS' drive and steering unit E/E/PE subsystems in case of a malfunction or be able to prevent those subsystems from influencing the trajectory. In either case, the system must be deployed – in dependence of the driving velocity and the heading – so that the trajectory cannot lead to exceeding the boundaries of the workspace. Using appropriate (time-variant and position-dependent) scaling factors in the MCA increases the availability of the WMDS. Controlling the trajectory relates to steering and/or accelerating and/or decelerating. Because decelerating is sufficient to transfer the WMDS into a safe state, easier to implement, lighter in weight, and safer in terms of reliability (compared to full control over the trajectory), an emergency braking system is favoured. Possible approaches to fulfil the requirements are formulated in a patent held by TU Dresden and AMST Systemtechnik (section 2.2.8.4) and have been designed and tested by TU Darmstadt, whereas the knee lever mechanism has been patented (section 7.3.3.1.1). Triggering the emergency braking system influences availability and safety, which is why the system should only be triggered if necessary. Therefore, several system states must be monitored, as described in section 7.2. A detailed analysis on how the integrity can be evaluated will be given in section 7.3.3.1.1.

7.3.1.2 Continuous Short Circuit Must be Avoided (SIL *3*)

A continuous short circuit can only arise from the power supply E/E/PE subsystem itself because only here energy is stored. Although energy can be generated by the electric motors during recuperation, this process is not continuous (limited kinetic energy is converted to electric energy and a rescue will only be initiated when MORPHEUS is in standstill) and is separately dealt with in section 7.3.1.3.

The safety function must monitor if there is a short circuit. This can be done by an Insulation Monitoring Device (IMD), e.g. the patented A-Isometer of the company Bender that measures the current between the reference ground and the insulated as well as active conductor. If the insulation resistance is below a predefined threshold, a short circuit is probable, and the power supply must be cut. For cutting the power supply, power contactors are needed.

7.3.1.3 HV Overvoltage Must be Avoided (SIL *3*)

HV overvoltage can arise from a malfunction in the power supply E/E/PE subsystem or from recuperation with the electric motors. Here, the safety function for the latter case is addressed because the power supply is monitored by its own safety certified BMS. Recuperation can be problematic because some types of accumulators can only absorb a fraction of the power that can be drawn from it.

The safety function must continuously monitor the current drawn from the electric motors during recuperation and limit this current to a value that is absorbable for the accumulator (20 A (DC) in MORPHEUS' setup). The safety function can easily be implemented in the motor controllers since the current to and from the electric motors is continuously measured and the controllers provide a function to limit the recuperation current[164]. If this risk reduction measure does not fulfil the safety integrity requirement sufficiently, a diode (e.g. surge protector) connected between the motor controllers and the traction battery can limit the power that must be absorbed by the accumulator.

7.3.1.4 AC/DC Converter Overvoltage Must be Avoided (SIL *2*)

In case of a malfunctioning AC/DC converter, an overvoltage at the mock-up E/E/PE subsystem might endanger the test person's health and that of subjects trying to rescue the test person as well if the overvoltage is continuous.

The continuous overvoltage safety function has already been addressed (section 7.3.1.2), thus, only very short overvoltage is possible until the IMD operates the power contactors. Then, the test person can be rescued without putting the rescue personnel at unreasonable

[164] E.g. UNITEK Industrie Elektronik GmbH: Manual Bamocar-D3 (2017).

risk. If this risk reduction measure does not fulfil the safety integrity requirement sufficiently, a fuse may limit the output power of the AC/DC converter to a safe value. Furthermore, a safety-certified AC/DC converter may be used.

7.3.1.5 Auxiliary Battery's Temperature Must be Monitored (SIL *2*)

If the temperature of the auxiliary battery is not monitored, overheating may not be detected, leading to short circuit and/or fire hazard.

(Continuous) short circuit has already been addressed (section 7.3.1.2). Auxiliary batteries with integrated temperature sensors are available on the market and must be introduced to the system. Thus, the safety function can be provided either by an automatic shutdown of the auxiliary battery in case of overheating (in this case power contactors must be integrated that can be operated by the auxiliary BMS) or manually by the system operator who would be obliged to monitor the auxiliary battery's temperature.

7.3.1.6 Water Ingress Must be Avoided (SIL *2*)

Water ingress is a safety issue for all components except for the surveillance system (coincidence of water ingress at surveillance system and a health issue of test person is very unlikely).

Instead of using waterproof components, which would contradict the lightweight concept, the occurrence of water should be avoided. On the one hand, the skilled operator can monitor the weather (when using MORPHEUS outdoors) and take precautionary countermeasures (e.g. driving MORPHEUS back into its hall). If the countermeasures have been taken too late, a sufficiently large, waterproof cover must be provided that can withstand the allowed wind speeds and can be appropriately secured so that MORPHEUS can endure wet weather. On the other hand, all subjects interacting with MORPHEUS must be instructed not to bring any liquids to the system (e.g. for drinking). Condensation, e.g. from the air conditioning, must be collected.

7.3.1.7 The Test Person Must be Able to Communicate with the System Operator and Vice Versa (SIL *2*)

The bidirectional communication between the test person and the system operator is important in case of health issues of the test person or if the situation is unclear to the test person. In the latter case, the test person could unbuckle and move within the dome while driving simulation is in progress.

The use of a safety-certified communication system could increase the availability. If the test person has a health issue, the system operator can still monitor the test person through the surveillance system. The test person must be instructed not to unbuckle under any circumstances until he or she is told to do so by the system operator. If these safety functions do not fulfil the safety integrity requirement sufficiently, the buckles could be remote controlled by the system operator so that the test person is not able to unbuckle him-

or herself. Of course, in case of a power cut, these automatic buckles would need a mechanical emergency release or be directly unlocked.

7.3.1.8 The Wireless Data Transmission Must Not Fail (SIL *2*)

Wireless data is transmitted between the external command device E/E/PE subsystem and the IPG Roadbox as well as the mock-up E/E/PE subsystem's communication and surveillance system.

If the emergency braking safety function (section 7.3.1.1) is implemented, the safety function can be reduced to "a wireless data dropout must be diagnosed". The diagnosis can be done by using more than one transmission channel and comparing the signals. If the number of transmission channels is sufficiently large, it is even possible to use the signals, if one channel fails.

7.3.1.9 Stationary Power Overvoltage Must be Avoided (SIL *1*)

In case of a stationary power overvoltage, the health of the system operator(s) might be endangered as well as that of subjects trying to rescue the system operator(s) if the overvoltage is continuous.

The continuous overvoltage safety function has already been addressed (section 7.3.1.2), thus only very short overvoltage is possible until the IMD operates the power contactors. Then, the system operator can be rescued without putting the rescue personnel at unreasonable risk. If this risk reduction measure does not fulfil the safety integrity requirement sufficiently, a fuse may limit the output power of the stationary power connector to a safe value.

7.3.1.10 Air Conditioning Must be Available (SIL *1*)

This safety function requirement was formulated in combination with water ingress at the air conditioning. If water ingress can be avoided, the safety integrity requirement drops to level a and, therefore, must not be accounted for.

7.3.1.11 The Test Person Must Remain Accessible (SIL *1*)

In case the hexapod cannot be operated (e.g. HV power cut, malfunctioning hexapod, etc.), the test person must remain accessible for rescue in any position of the hexapod.

This safety function can be fulfilled by providing a ladder or some other kind of mobile entry aid. In MORPHEUS' current setup, the height of the entrance to the dome is about 1 m above floor level. Even if the dome is fully tilted (18°) and at maximum heave (75 mm), this would result in an entrance level of about 1.5 m.

7.3.1.12 Nobody Must be Injured or Killed if the Dome Becomes Loose or Instable (SIL *1*)

In case of a malfunction within the hexapod E/E/PE subsystem, it might happen that – due to mechanical stress because of a violation of the inverse kinematics model's integrity

– one or more actuators fail, and the dome becomes instable so that the position and motion cannot be controlled. In a worst-case scenario, the remaining actuators cannot bear the static and dynamic load of the dome so that the dome becomes entirely loose and might fall off the self-driving platform. These hazards can endanger system engineer(s) and/or mechanic(s) during maintenance or test drives as well as the test person during regular driving simulation.

The safety function must be able to prevent the dome from falling off the self-driving platform in any case. Strengthened actuators and actuator mounts could achieve this. Another option is to utilise restraining straps that only come into effect if the maximum stroke of the actuators is exceeded. Thus, the position can be controlled to some extent but high accelerations and the risk of crushing (a) system engineer(s) and/or mechanic(s) are still present. Using actuators with a self-locking effect cannot prevent unwanted motion because already one malfunctioning actuator makes one DOF uncontrollable. In any case, the system engineer(s) and mechanic(s) must be instructed to stand back of the hexapod and self-driving platform as soon as power is supplied to the hexapod, steering unit, or drive unit E/E/PE subsystem. In addition, putting a bellows over the hexapod reduces the risk of being crushed significantly.

7.3.2 Overall Safety Architecture

An **external emergency braking system** is employed that disconnects the tires from the underground, supplies its own energy, and is triggered either by a safety logic or manually by the system operator. The safety logic itself must be programmed in a fail-safe manner, e.g. in a programmable logic controller, and in such a way that emergency braking is triggered as soon as the programmable logic controller does not send an “OK”-signal. Analysing the revised HARA, with all safety functions implemented except the external emergency braking system, revealed that the following states must be monitored with the outlined safety integrity requirements:

- Malfunctioning of (SIL *1*)
    - AC/DC converter
    - measurement unit for motion quantities
    - auxiliary battery
    - electric motor
    - external command device
    - central control unit
    - motor controller
    - traction battery
    - stationary power connector

- HV overvoltage from the traction battery to steering and/or drive unit E/E/PE subsystems' motor controllers (SIL *2*)
- HV overvoltage from the steering or drive unit E/E/PE subsystems' motor controllers to the traction battery (recuperation) (SIL *1*)
- HV power cut between the traction battery and the steering and (SIL *2*)/or (SIL *1*) drive unit E/E/PE subsystems' motor controllers
- LV overvoltage from the auxiliary battery to steering and/or drive unit E/E/PE subsystems' motor controllers and/or WMDS dynamics control E/E/PE subsystem (SIL *1*)
- LV power cut between the auxiliary battery and the steering and (SIL *2*)/or (SIL *1*) drive unit E/E/PE subsystems' motor controllers
- LV power cut between the auxiliary battery and the WMDS dynamics control E/E/PE subsystem (SIL *2*)
- AC/DC converter overvoltage (SIL *2*)
- Stationary power connector overvoltage (SIL *1*)
- Stationary power connector power cut (SIL *2*)
- Faulty data transmission between the central control unit and the
    - Auxiliary battery (SOC) (SIL *2*)
    - Traction battery (SOC) (SIL *2*)
    - External command device (SIL *2*)
    - Drive unit's motor controllers (SIL *2*)
    - Steering unit's motor controllers (SIL *1*)
    - measurement unit for motion quantities (SIL *1*)
- Incorrect data from the measurement unit for motion quantities (SIL *2*)

Especially for wireless data transmission, at least two channels must be employed, making a diagnosis possible. The MCA must be adapted so that the driving velocity is sufficiently low that emergency braking is always possible without leaving the workspace.

An **IMD** monitors the insulation integrity and operates power contactors in the power supply E/E/PE subsystem if a short circuit is detected. An **additional power contactor** is integrated into the auxiliary battery and can be operated by the auxiliary battery's BMS. The auxiliary battery itself is replaced by a version with integrated **temperature sensors**. **Fuses** between motor controllers and traction battery, between the AC/DC converter and the mock-up E/E/PE subsystem, and between the stationary power connector and the external command device prevent overloads. The **recuperation current** from the electric motors is **limited** within the motor controllers to a value that is absorbable for the accumulator.

A sufficiently large, waterproof **cover** must be provided to the system operator(s) to avoid water ingress in case of sudden weather changes. In addition, a sufficiently large **ladder**

or other kind of entry aid must be provided to be able to rescue the test person from the dome if the hexapod is not operable.

The hexapod is put into a **bellows** to prevent anybody from being crushed. **Restraining straps** prevent the dome from falling off the self-driving platform if more than one actuator breaks.

The **conduct guidelines** prohibit all subjects interacting with MORPHEUS from bringing liquids into the system. Furthermore, the test person must be instructed not to unbuckle under any circumstances unless he or she is told to do so by the system operator. System engineers and mechanics must be instructed to stand back of the system when HV is switched on unless direct contact with the system is absolutely essential. The system operator(s) is/are required to monitor the weather if MORPHEUS is used outdoors so that countermeasures can be taken at an early stage if wet weather occurs and to monitor MORPHEUS' workspace for unauthorised subjects. He or she is also instructed to drive with low velocity in manual mode when MORPHEUS is close to its workspace boundaries and to thoroughly check MORPHEUS' workspace for obstacles prior to the initialisation of a driving simulation.

Revising the HARA revealed that the following safety functions must be implemented, too, for reducing all hazards to a SIL of *a*: **Self-programmed software**, especially for the MCA and MC, must be externally **reviewed** and thoroughly **tested** before putting into operation. If this measure will not fulfil the safety integrity requirement, an outer software layer could be implemented that monitors only the very safety-relevant information (e.g. absolute position in workspace and target vs. actual motion) and can directly activate the external emergency braking system. The **HV accumulator and its BMS** – although safety-oriented – must provide a **high availability** so that a shutdown of the HV power supply is unlikely.

The full list of revised hazards can be found in annexe C.3, where all hazardous events have been evaluated with a SIL of *a*.

7.3.3 Exemplary Application of the Safety Architecture

In this section, a specific, exemplary application of the safety architecture will be evaluated in regard of its functional safety. The application includes the safety functions external emergency braking E/E/PE system and the IMD E/E/PE element.

7.3.3.1 Determination of the Limits of Machinery

The users, uses cases, and environment are identical with those of MORPHEUS (cf. sections 7.1.1.1, 7.1.1.2, and 7.1.1.4).

7.3.3.1.1 External Emergency Braking E/E/PE Subsystem

Although mechanically mounted to the WMDS, the emergency braking safety function is implemented externally and, therefore, supplies its own energy for the activation of the emergency braking. The system is connected to an IPG Roadbox as well as a manual emergency stop through CAN and is fed by a LV power supply that is not needed for activating an emergency braking.

The **external emergency braking E/E/PE subsystem** is designed to lift MORPHEUS off the ground so that the tires lose contact to the underground[165,166]. The friction partners, namely road surface and the emergency braking system's brake pads, are designed in such a way that the friction coefficient is equal or below that of MORPHEUS' tires to the road surface, thus preventing overturning. The energy for deploying the safety system is stored in steel coil springs (hazardous element) that are preloaded when the safety system is engaged. Electric holding magnets (actuator) that are powered by the on-board auxiliary batteries (LV) counteract the preloaded springs. Contact switches are used in each safety system, detecting whether the system is engaged or deployed. When the safety system is triggered, which may be done either manually or automatically by a programmable logic controller (initiating mechanism), the magnet's energy supply is cut, and the preloaded springs push the brake pads against the road surface, lifting MORPHEUS off the ground. A knee lever is installed for transforming the required vertical force acting on the brake pads to a desired shape and has been patented[167]. Dampers are installed for controlling the system's dynamics and iteratively tuned to the desired behaviour. The undamped vertical force of the emergency braking system was sufficiently large to make MORPHEUS jump and, thus, generated unwanted large vertical accelerations and mechanical stress. Figure 7-7 shows the CAD model of the emergency braking system, whereas the left system is engaged, and the right system is deployed. Figure 3-4 shows a photograph of the emergency braking system on MORPHEUS.

---

[165] Betz, A. et al.: Development and Validation of a Safety Architecture of a WMDS (2014).

[166] Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). pp. 81-89.

[167] Betz, A.; Winner, H.: Patent Knee Lever Safety System (2014).

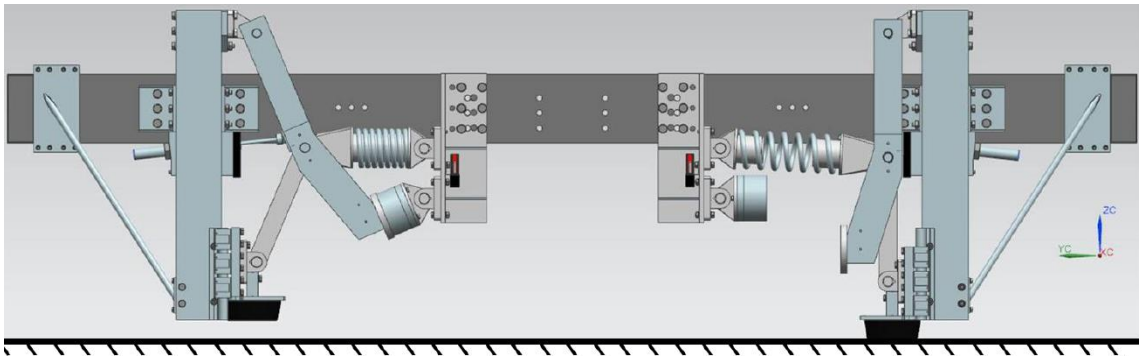

Figure 7-7: Emergency braking system. Left: Engaged, right: Deployed

An essential function of the external emergency braking system is monitoring the integrity of MORPHEUS. Therefore, the following information are gathered in the programmable logic controller:

- IMDs detect short circuits and overvoltage between
  - Traction battery and steering and/or drive unit's motor controllers and/or hexapod's power electronics
  - Auxiliary battery and steering and/or drive unit's motor controllers and/or WMDS dynamics control E/E/PE subsystem
  - AC/DC converter and mock-up E/E/PE subsystem (this is the only function of the AC/DC converter and, therefore, also constitutes its malfunction)
  - Stationary power connector and external command device E/E/PE subsystem (this is the only function of the stationary power connector and, therefore, also constitutes its malfunction)
- Motor controllers send error codes in case of
  - Malfunctioning electric motor (measurement of speed and temperature)
  - Malfunctioning motor controller (self-diagnosis)
  - Overvoltage from steering or drive unit's electric motors (recuperation)
  - HV power cut between traction battery and steering and/or drive unit's motor controllers
  - LV power cut between auxiliary battery and steering and/or drive unit's motor controllers
- IPG Roadbox sends error codes in case of
  - Malfunctioning ADMA G-3 (self-diagnosis)
  - Malfunctioning steering or drive unit (comparing target motion and actual motion)
  - Erroneous ADMA G-3 signals (measurement and data transmission; plausibility of the signals is checked by comparing to an inertial measurement unit (IMU) that is redundantly integrated into the WMDS dynamics control E/E/PE subsystem)

    - Malfunctioning traction BMS
    - Malfunctioning auxiliary BMS
    - Erroneous battery SOC signals (measurement and data transmission; plausibility of signal must be checked when initialising driving simulation, then the SOC signal's plausibility can be checked with the WMDS energy model)
    - Malfunctioning IPG Roadbox (self-diagnosis)
    - LV power cut between the auxiliary battery and the WMDS' dynamics control E/E/PE subsystem
    - Faulty data transmission between the IPG Roadbox and external command device (at least two wireless channels are employed and can be compared, checksums and/or watchdogs assure that valid signals are sent)
    - Faulty data transmission between the IPG Roadbox and the motor controllers (checksums and/or watchdogs assure that valid signals are sent)
- External command device sends error codes or no "OK"-signal in case of
    - Malfunctioning external command device (self-diagnosis)
    - Power cut between stationary power connector and external command device E/E/PE subsystem
- Manual emergency stop that is operated by system operator(s)
- Contact switches at each knee lever detect if one knee lever is unintentionally activated

All information (also "OK"-signals) must be sent within predefined time intervals. If one piece of information does not reach the programmable logic controller in time, emergency braking is activated.

Figure 7-8 gives an overview of the functional safety-relevant components that are included in the external emergency braking E/E/PE system, whereas the italic labels represent information and arrows indicate the direction of flow of power and information signals:

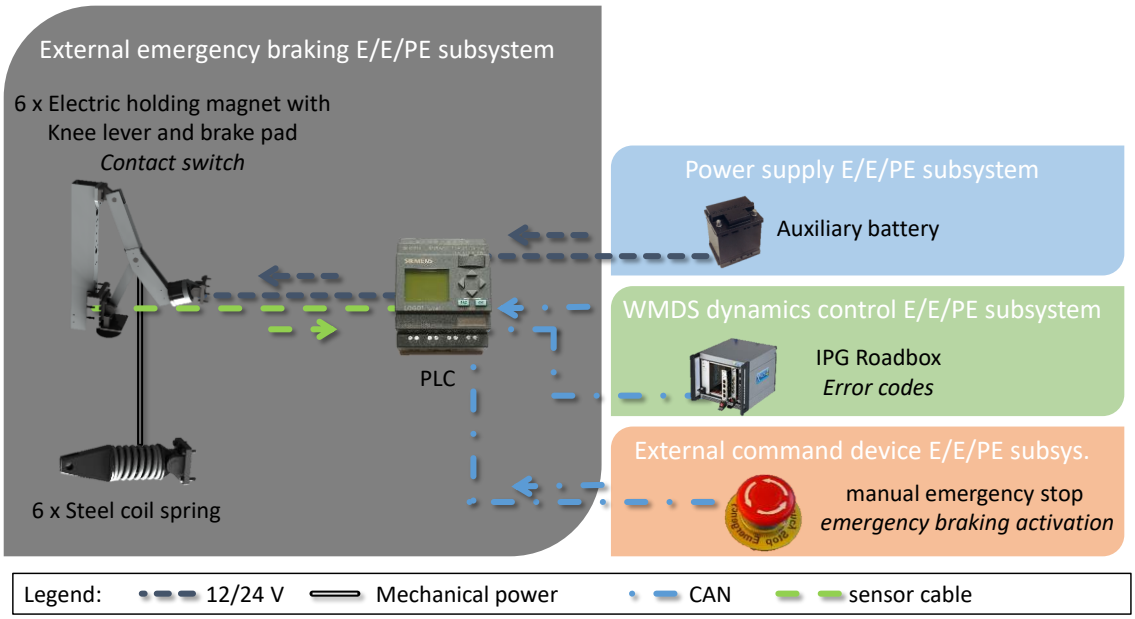

Figure 7-8: MORPHEUS' external emergency braking E/E/PE system

7.3.3.1.2 Revised Power Supply E/E/PE Subsystem

The IMDs (sensors) are implemented into the **power supply E/E/PE subsystem** and measure the current between the reference ground and the insulated as well as active conductors of all energy sources (hazardous element). The auxiliary battery's and the AC/DC converter's IMDs send their information to the auxiliary BMS (electronic control unit), the traction battery's IMD to the traction BMS (electronic control unit) and the stationary power connector's IMD to a switch located between the stationary power connector and its IMD. If a short circuit or undervoltage is measured, the corresponding power contactors (actuator) of the batteries or the switch (actuator) in the stationary power supply are operated and power is cut. Overvoltage is avoided by the implementation of fuses and limiting the recuperation current in the motor controllers. The IMDs are supplied with 12 V (DC).

Figure 7-9 gives an overview of the components that are included in the revised power supply E/E/PE system, whereas the italic labels represent information and arrows indicate the direction of flow of power and information signals:

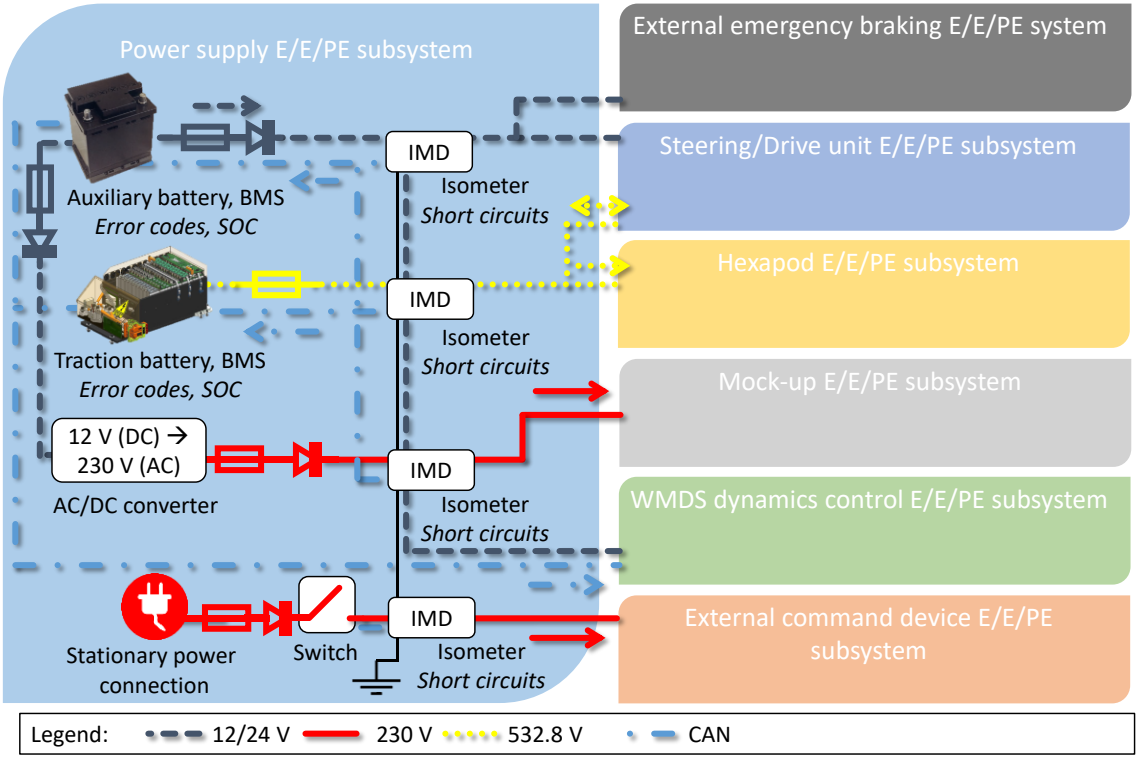

Figure 7-9: MORPHEUS' revised power supply E/E/PE subsystem

7.3.3.2 Hazard Identification & Risk Estimation

The hazard list with 21 additional, evaluated combinations of failures, consequences, and situations for the exemplary application of the safety architecture is attached in annexe C.4.

7.3.3.3 Risk Evaluation & Safety Requirements

The following safety requirements are established from the hazard list:

- System engineer(s) and/or mechanic(s) must not be injured or even killed when working at the WMDS and emergency braking is activated (SIL *1*)
- Short circuit must be reliably detected by IMDs (SIL *a*)
- LV power supply must not be cut (SIL *a*)
- LV power supply must not exceed nominal voltage (SIL *a*)
- Fuses must reliably blow at threshold current (SIL *a*)
- Electric holding magnet must not provide no or too low/high force (SIL *a*)
- Steel coil springs must always be preloaded prior to driving simulation initialisation (SIL *a*)

Therefore, it is proposed to build a housing around the emergency braking system so that nobody can be crushed or be injured otherwise by the system. The conduct guidelines are appended by the instruction that the system operator must check the emergency braking

system visually prior to initialising driving simulation. Especially checking if all steel coil springs are preloaded is mandatory.

7.4 Adaption to Full-Scale WMDS

Besides the design changes in terms of size, weight, power, and energy supply, as described in section 3.6, changes in the safety architecture are necessary as well when building a full-scale WMDS. The external emergency braking system can be kept, although adapted in size and power to be able to handle the increased wheel load. The electric architecture with IMDs and fuses can be kept, too. The increased size makes it difficult to use a waterproof cover in case of sudden weather changes. Either the full-scale WMDS is constructed in such a way that the system is at least safe in wet conditions when it is shut down or some kind of aid must be provided to cover the WMDS in all possible emergency states and under all environmental conditions. Because of the increased size and the expectable stroke increase of the hexapod, it will become more difficult to rescue the test person from the dome in case of emergency and power cut. Also, the WMDS' workspace will probably increase, making it even more time consuming to reach the test person on foot. A possible solution could be derived from passenger boarding stairs as used in aviation (a.k.a. boarding ramps or stair car). This approach could also be used for regular entrance to the dome, if mobile stairs is equipped with a top platform that is adjustable in height. A solution that is easier to implement are inflatable emergency slides as also used in aviation that come into action in case of emergency. If the full-scale WMDS is intended to be used with more than one test person simultaneously, a thorough revision of the HARA must be conducted because many safety integrity requirements resulted of the assumption that only one person can be injured or killed in the dome.

7.5 Discussion

A suitable safety architecture for WMDS in general has been found and theoretically demonstrated to reduce risk to an acceptable level. It was surprising to find out that no environment perception is required when subjects are restrained from entering the WMDS' driving area. Although the implementation of an external emergency braking system comes to mind somewhat intuitively, this safety measure is demanded by a vast number of safety requirements. Furthermore, the importance or the communication between test person and system operator could intuitively be underestimated.

Concluding, the hypothesis H1.2 *cannot be falsified*, considering the determined limits of the WMDS, international functional safety standards, and state-of-the-art-technology.

8 Conclusion

The results presented within this thesis provide the next building block towards proving general feasibility of WMDS. The falsification aspects power demand, energy demand, and latency are practically researched in experiments and the falsification aspect safety architecture in theory, trying to falsify the working hypotheses H1.1 and H1.2 (sections 1.2.3.1 and 1.2.3.2).

8.1 Wheeled Motion Base

> H1.1: "The wheeled motion base of [FZD's] WMDS [concept] with its dynamics limited by friction forces can simulate the horizontal dynamics of urban traffic for normal driver behaviour considering common scaling factors" [168].

The falsification aspect **power demand** is researched with a verified power model. The model is designed partially based on physical effects (power demand by mass moment of inertia, self-alignment torque, and drill torque) and partially based on empirical findings where the underlying physical effects were so complex that a detailed model would not justify the effort required for modelling and parameterisation (driving resistance, steering holding power, and electrical efficiency). The parameterisation is done with coasting experiments (driving resistance model), steering holding torque experiments (steering holding power), and straight-line acceleration experiments (electrical efficiency). The parameterised model is then verified by conducting straight-line driving manoeuvres with constant acceleration with MOPRHEUS while measuring the current and voltage at the accumulator and comparing the experimental with the simulative results. The verified model is then used to determine the power demand for different scaling factors. MORPHEUS' current setup can provide driving simulation up to scaling factors of 0.7. For unscaled driving simulation, the electric motor power is sufficient, but the accumulator's power must be increased by the factor three. Thus, the aspect power demand is **not able to falsify hypothesis H1.1**.

The falsification aspect **energy demand** is researched with a validated energy model that is derived from the power model. The parameterised model is validated by driving a 90°-turn, a figure eight, and a scaled representative urban driving circuit with

[168] Cf. Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015). p. 4.

MORPHEUS. The validated model is then used to simulate the energy demand in unscaled urban driving scenarios for the fully set-up MORPHEUS prototype. The highest resulting average energy demand is extrapolated to the demanded 2 h experiment duration. Auxiliary energy consumers are measured and added to the energy demand by the motion system. Although the accumulator used in MORPHEUS is not able to fulfil the requirement, state-of-the-art accumulators are. Then, the accumulator's energy must be increased by the factor five, including the additional energy demand by the mass increase. Thus, the aspect energy demand is **not able to falsify hypothesis H1.1**.

The falsification aspect **latency** is researched by imposing step inputs to MORPHEUS. The experimental design is chosen so that the influence of the initial driving velocity, the acceleration step input amplitude, and the type of control (acceleration and steering angle step input) are considered. Whereas the acceleration step input amplitude showed no influence on latency if the indicator for latency is independent of the amplitude, the initial driving velocity has a significant influence. Motion latency shows the highest value at low driving velocities and asymptotically decreases at higher velocities. The steering angle step input showed marginally higher latency than the acceleration step input. Considering inaccuracies in the measurement, this influence can be neglected. Concluding, the highest $ACL_{50\,\%}$ was found at 7 m/s² acceleration step input amplitude and 0 driving velocity with a value of 159 ms, which is above the requirement of 135 ms. The highest ACL_{gain} was found at 6 and 7 m/s² acceleration step input and 0 driving velocity with a value of 104 ms, which is slightly above the requirement of 100 ms. Considering the control approach of keeping the WMDS in motion, the restrictive requirement for $ACL_{50\,\%}$, and the small deviation from the requirement, the aspect latency is **not able to falsify hypothesis H1.1**.

8.2 Safety Architecture

H1.2: FZD's WMDS concept does not bear an unacceptable risk to a human under any environmental conditions and in any use case.

The falsification aspect of a **safety architecture** is investigated by conducting a HARA, formulating safety requirements, and proposing a safety architecture design that fulfils these requirements. The HARA yields 186 hazardous events that are addressed by twelve main safety requirements, whereas the most important requirement is that the DS trajectory must remain controllable so that collisions with objects and subjects can be avoided with a SIL of *4*. Five safety requirements address electrical safety (continuous short circuit must be avoided (SIL *3*), HV overvoltage because of recuperation must be avoided (SIL *3*), AC/DC converter overvoltage must be avoided (SIL *2*), auxiliary battery's temperature must be monitored (SIL *2*), and stationary power overvoltage must be

avoided (SIL *1*)). Furthermore, water ingress at all E/E/PE systems must be avoided (SIL *2*), the test person must be able to communicate with the system operator and vice versa (SIL *2*), the wireless data transmission must not fail (SIL *2*), the test person must remain accessible (SIL *1*), and nobody must be seriously injured or killed if the dome becomes loose or instable (SIL *1*).

Being able to control the WMDS' trajectory with the on-board power supply and actuators under any given circumstances requires a tremendous effort in designing functions, signal transmission, and software to fulfil the safety integrity requirement. Thus, the decision is made for an external risk reduction facility, namely an emergency braking system, because this concept represents the easiest and thereby the safest way to control the trajectory (in terms of reliability in comparison to a risk reduction facility intended to keep full trajectory control over the WMDS). Monitoring all failures that require the emergency braking system to be triggered is crucial. The electrical safety requirements are addressed by implementing IMDs that control power contactors, limiting the recuperation current in the motor controllers, implementing diodes and fuses, and by utilizing an auxiliary battery with integrated temperature sensors. A multichannel wireless data transmission is introduced. A weatherproof cover for the WMDS and a ladder for emergency evacuation from the dome must be provided. The hexapod must be secured by restraining straps and bellows must be installed. All other safety requirements can be addressed by conduct guidelines.

The architecture is verified by re-assessing the hazardous events and by assessing the risk for the newly introduced function and components. No hazardous events are identified that require a risk reduction, thus, the architecture is able to fulfil the safety requirements for a WMDS. Concluding, the falsification aspect of a safety architecture for WMDS is **not able to falsify hypothesis H1.2**.

8.3 Outlook

Although hypothesis H1.1 and H1.2 were not falsified, it could not be ultimately proven that they are practically valid. For hypothesis H1.1 this ultimate proof would imply installing sufficient accumulators for fulfilling the power and energy demand, increasing the platform's maximum velocity, and implementing the control approach of keeping the WMDS in motion. For hypothesis H1.2 this ultimate proof would require implementing the designed safety architecture into MORPHEUS. Although the emergency braking system has already been installed on MORPHEUS and proven reliable, though sensitive, no statistical evidence is provided. Not to mention the remaining safety functions.

Measurements revealed that due to vertical excitation from the uneven road surface and, also, because of the lack of a suspension on MORPHEUS the wheel load fluctuation becomes so large at high velocities that the average friction coefficient is impaired. Besides a solution by a very even pavement for operation, a vertical dynamics control of a WMDS, as currently researched by Zöller[169], is assumed to resolve this problem. Furthermore, the signal quality in general would profit from reduced vertical excitation, as – most importantly – would the immersion of the test person, too.

Of course, all falsification aspects have been researched with the scaled prototype MORPHEUS. For the power and energy demand, no direct conclusions can be drawn for the full-scale WMDS, because design changes would affect the validity of the power/energy model. Still, the found results increase the confidence in the feasibility of these aspects. Latency is not expected to change significantly, especially with the novel control approach. Also, for a full-scale WMDS the HARA must be revised, and the safety architecture adapted to the updated safety requirements. Although specific for MORPHEUS, the extensively conducted HARA provides a basis for assessing the risk of any WMDS. Although these findings suggest that the falsification aspects will also not be able to falsify the working hypotheses in a full-scale WMDS, the practical evidence is to be provided. Thus, designing and building a full-scale WMDS with a system to control the vertical excitation induced by uneven driving surfaces and the updated safety architecture applied to it is the next consequent step in FZD's WMDS project. This full-scale WMDS would be able to evaluate the immersion of the test person that can be accomplished with the concept in comparison to state-of-the-art DS and, therewith, assumingly prove overall practical feasibility and the claimed advantages of WMDS.

[169] Zöller, C. et al.: Tires and Vertical Dynamics of WMDS (2017).

A Overturning Stability[170]

In case of full acceleration, it must be ensured that the WMDS will not turn over. Overturning will start as soon as one of the wheel loads gets smaller than zero. Within a defined triangle, Figure 8-1 left, safety against overturning is assured by setting up the free body diagram, Figure 8-1 right, and calculating the momentum equilibrium around point 2, wherein COG is the abbreviation for Centre Of Gravity:

$$\sum_{(2)} T = 0 = m_{\mathrm{DS}} \cdot g \left(\mu_{\mathrm{tire}} \cdot h_{\mathrm{COG}} - h_{\mathrm{COG,t}}\right) + h_{\mathrm{t}} \cdot F_{z,\mathrm{W,rear}} \tag{8-1}$$

For the overturning stability of MORPHEUS, this triangle is defined as the equilateral triangle that is spread out by the tire's contact points to the road surface. Applying the geometric relations, which can be derived from Figure 8-1 left, overturning stability is ensured by complying with inequality (8-3):

$$F_{z,\mathrm{W,rear}} = \frac{2\, m_{\mathrm{DS}} \cdot g \left(\frac{1}{2\sqrt{3}} l_{\mathrm{t}} - \mu_{\mathrm{tire}} \cdot h_{\mathrm{COG}}\right)}{\sqrt{3} l_{\mathrm{t}}} > 0 \tag{8-2}$$

$$\rightarrow l_{\mathrm{t}} > 2\sqrt{3}\mu_{\mathrm{tire}} \cdot h_{\mathrm{COG}} \tag{8-3}$$

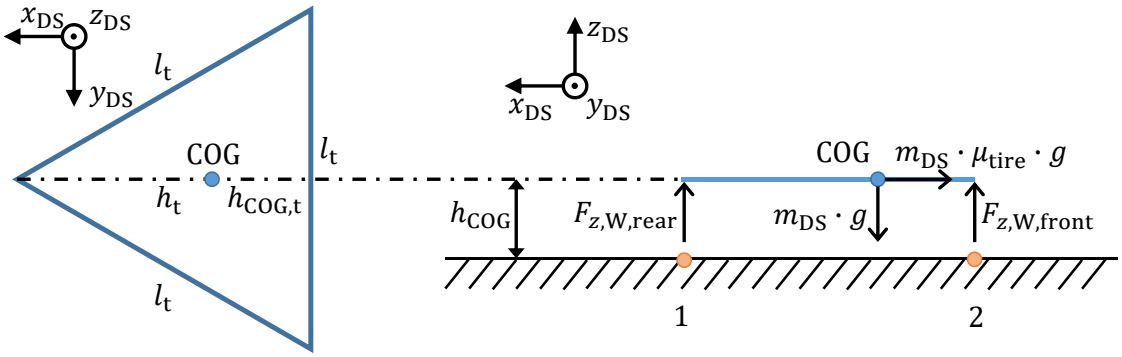

Figure 8-1: Left: Geometry of omnidirectional motion base; Right: Balance of forces of the omnidirectional motion base when accelerating

This makes it obvious that overturning protection is only dependent upon friction coefficient, height of the triangle, and height of COG. The height of MORPHEUS' COG h_{COG} is 481 mm; the length of the triangle edges l_{t} is 2,300 mm. Applied to equation (8-3), this results in a maximum possible acceleration before overturning:

$$l_{\mathrm{t}} = 2\sqrt{3}\, \frac{a_{\mathrm{DS,hor,max}}}{g} \cdot h_{\mathrm{COG}} \tag{8-4}$$

[170] Wagner, P. et al.: Conception and Design of Mobile Driving Simulators (2014). pp. 5, 8.

$$\rightarrow\ a_{\mathrm{DS,hor,max}} = \frac{g\ l_{\mathrm{t}}}{2\sqrt{3}\ h_{\mathrm{COG}}} = 13.54\ \frac{\mathrm{m}}{\mathrm{s}^2} \tag{8-5}$$

Since the friction coefficient of the used press-on band tires on regular road surfaces is limited to approximately 0.8[171,172], safety against overturning is assured for friction traction.

[171] Betz, A. et al.: Konzeptanalyse und Erprobung eines WMDS (2014).

[172] Zöller, C. et al.: Tire Concept Investigation for WMDS (2016).

B Experiment Results

B.1 EMRAX 228 Electric Motor Efficiency Map According to Enstroj

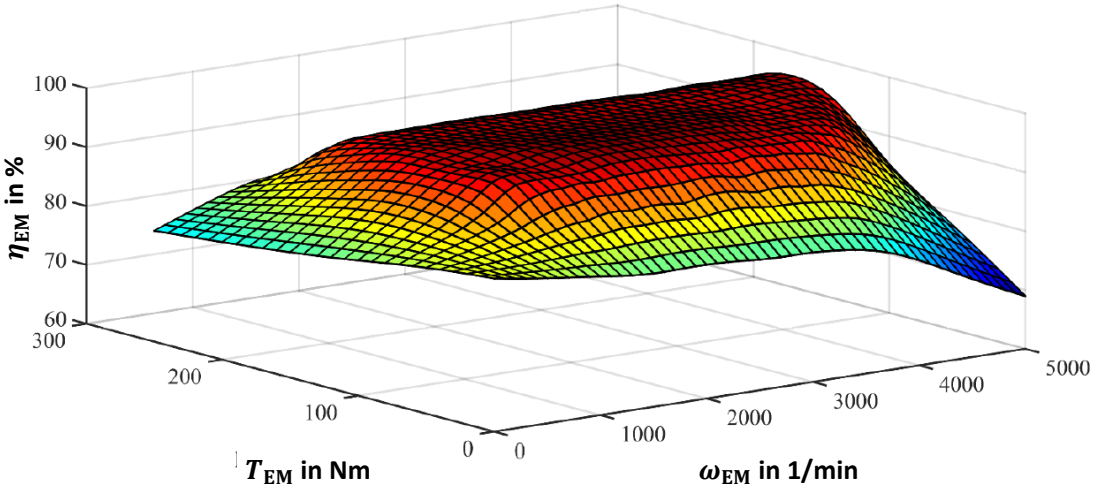

Figure 8-2: Linearly interpolated efficiency map of the EMRAX 228 according to data provided by Enstroj[173]

[173] Albrecht, T. et al.: Advanced Design Project, Fahrwiderstands- und Energiebedarfsbetrachtung des MORPHEUS (2016). p. 47.

B.2 Variation of Acceleration Amplitude

The table shows the ACL in ms, caused by varied lateral acceleration step inputs, calculated with the $IACL_{50\,\%}$ and $IACL_{gain}$, and driven with initial longitudinal driving velocities of 0 and 1 m/s. The values for ACL are averaged over six trials. For the ACL_{gain} the relative MSD is calculated

	v_0 in m/s	$a_{lateral}$ in m/s²								MSD_{rel}
		1	2	3	4	5	6	7	8	
$ACL_{50\,\%}$ in ms	**0 m/s**	123	134	145	150	155	155	**159**	157	-
	1 m/s	81	93	101	113	122	127	134	139	-
ACL_{gain} in ms	**0 m/s**	102	95	98	84	89	**104**	**104**	77	17.4 %
	1 m/s	59	59	55	58	56	53	66	56	10.9 %

B.3 Variation of Initial Velocity

The table shows the ACL in ms, caused by a 5 m/s² lateral acceleration step input or 90° steering angle step input, calculated with the $IACL_{50\,\%}$ and $IACL_{gain}$, and driven with varied initial longitudinal driving velocity. The values for ACL are averaged over six trials.

Step input	**ACL**	v_0 in m/s						
		0	1	2	3	4	5	6
$a_{target} = 5\ \frac{m}{s^2}$	**$ACL_{50\,\%}$ in ms**	**155**	122	100	97	78	83	78
	ACL_{gain} in ms	**89**	56	46	32	34	35	46
$\delta_{target} = 90°$	**$ACL_{50\,\%}$ in ms**	-	**121**	110	118	114	119	120
	ACL_{gain} in ms	-	**65**	48	53	52	48	44

C Safety Analysis

C.1 List of Built-in Components

Legend:

	Purchased part
	Milled part
	Turned part
	Part used in earlier version

Part Number	Qty.	Part name	Supplier, Material, Dimension
1	3	Cross-roller bearing	Kistenpfennig
2	3	Crossbeam bearing	JHW, X37CrMoV5-1, plate 180,4 x 25,4 mm, 1 m
3	3	Strut wheel hub	JHW, X37CrMoV5-1, plate 200,4 x 20,4 mm
4	3	Wheel hub	BMW
5	3	Adapter wheel hub	Geier, EN AW 6082 T6 round rod 200 mm
6-8	3	Compensation coupling	KTR
9	3	Adapter gearbox	Geier, EN AW 6082 T6 round rod 100 mm
10	3	Rim	Pneuhage
11	3	Tyre	Gumasol
12	3	Sleeve gearbox	Bieber+Marburg, S355 round tube 244,5 x 50 mm
13	6	Gearbox	Neugart
14	3	Strut gearbox	JHW, X37CrMoV5-1, plate 200,4 x 6,2 mm
15	3	Strut drive	JHW, X37CrMoV5-1, plate 200,4 x 15,4 mm
16	6	Adapter electric motor	Geier, EN AW 6082 T6 round rod 100 mm
17	3	Crossbeam drive	JHW, X37CrMoV5-1, plate 200,4 x 15,4 mm
18	3	Electric motor	Enstroj
19	3	Strut electric motor	JHW, X37CrMoV5-1, plate 200,4 x 6,2 mm
20	3	Adapter gearbox 2	Geier, EN AW 2007 round rod 200 mm x 34 mm
21	3	Flange slip ring	Geier, EN AW 2007 round rod 150 mm x 18 mm
22	3	Flange spline shaft	Mädler
23	3	Slip ring	Rie-Tech
24	3	Bracket electric motor	Alu Boll, EN AW 7075, eroded to outer contour
25	9	Strut steering frame	Geier, EN AW 2007 flat bar, 30 mm x 12 mm, 220 mm
26	3	Bracket gearbox	Geier, EN AW 2007 round rod 270 mm x 10 mm
27	3	Sleeve steering frame	Metallstore, Alu, tube 250 mm x 20 mm, 200 mm

Part Number	Qty.	Part name	Supplier, Material, Dimension
28	3	lower frame plate	Geier, Alu, plate >273 x 20 mm, 500 mm
29	3	upper frame plate	Geier, Alu, plate >273 x 20 mm, 500 mm
30	3	Crossbeam frame	Alu Boll, EN AW 6060, rectangular tube 150x100x3
31	3	Strut frame	Geier, EN AW 6060 T66 (AlMgSi0,5), rectangular tube 100x50x2
32	3	Supporting strut steering frame	Alu round rod 15 mm x 150 mm
33	3	Left inner flange steering frame strut	Geier, EN AW 6060, elbow 50 mm x 50 mm x 5 mm
34	3	Right inner flange steering frame strut	Geier, EN AW 6060, elbow 50 mm x 50 mm x 5 mm
35	6	lower flange steering frame	Geier, EN AW 6060, flat bar 150 mm x 10 mm
36	6	outer flange steering frame	Geier, EN AW 6060, elbow 120 mm x 80 mm x 10 mm
37	6	Strut hexapod	Geier, EN AW 6060 T66 (AlMgSi0,5), rectangular tube 100x100x2
38	6	Right flange hexapod strut	Geier, EN AW 6060, elbow 50 mm x 50 mm x 8 mm
39	6	Left flange hexapod strut	Geier, EN AW 6060, elbow 50 mm x 50 mm x 5 mm
40	3	Outer flange Hexapod strut	Geier, Alu, plate 150 x 10 mm, 500 mm
41	3	Left outer flange hexapod	Geier, EN AW 6060, elbow 50 mm x 50 mm x 8 mm
42	3	Right inner flange hexapod	Geier, EN AW 6060, elbow 50 mm x 50 mm x 8 mm
43	3	Left inner flange hexapod	Geier, EN AW 6060, elbow 50 mm x 50 mm x 8 mm
44	3	Right outer flange hexapod	Geier, EN AW 6060, elbow 50 mm x 50 mm x 8 mm
45	1	Hexapod	MeVEA
46	12	Inner insert frame bar	Geier, EN AW 2007, flat bar 144 mm x 100 mm x 20 mm
47	6	Middle insert frame bar	Geier, EN AW 2007, flat bar 94,5 mm x 100 mm x 20 mm
48	24	Outer insert frame bar	Geier, EN AW 6082 T6 round tube 20 mm x 5 mm, 144 mm
49	18	Insert frame strut	Geier, EN AW 6082 T6 round tube 20 mm x 5 mm, 46 mm
50	36	Inert hexapod strut	Geier, EN AW 6082 T6 round tube 20 mm x 5 mm, 96 mm
51	6	Power electronics	UniTek
52	3	Bracket power electronics	Alu Boll, EN AW 6082, eroded to outer contour
53	1	Mounting aid drive unit	Stock item
54	3	Rotation lock slip ring	Geier, EN AW 2007 flat bar, 30 mm x 12 mm
55	3	Spacer slip ring	Geier, EN AW 2007, disc 180 mm x 17 mm
56	3	Rubber buffer	Wagner Verbindungstechnik
57	3	Cover frame corner	Geier, EN AW 2007, plate 340 mm x 190 mm x 6 mm
58	3	Safeguard frame corner	Alu Boll, EN AW 5754, eroded to outer contour

Part Number	Qty.	Part name	Supplier, Material, Dimension
59	3	Support safeguard frame corner	Alu Boll, EN AW 6060, flat bar 30 mm x 12 mm
60	3	Flange safeguard frame corner	Alu Boll, EN AW 6060, elbow 50 mm x 50 mm x 5 mm
61	6	SaSy Lever L1	Alu Boll, EN AW 6082, flat bar 40 mm x 15 mm x 310 mm
62	6	SaSy Lever L2	Alu Boll, EN AW 6060, rectangular tube 60 mm x 40 mm x 4 mm
63	6	SaSy Lever L3	Alu Boll, EN AW 6060, rectangular tube 60 mm x 40 mm x 4 mm
64	12	SaSy reinforcement Lever L2	Alu Boll, EN AW 7075, plate 70 mm x 52 mm x 6 mm
65	12	SaSy connection lever L2-L3	Alu Boll, EN AW 7075, plate 240 mm x 120 mm x 6 mm
66	18	SaSy bearing block lever L2	Mädler
67	6	SaSy bearing block lever L3	Mädler
68	6	SaSy linear slide bearing DryLin W	igus
69	6	SaSy spring	Knörzer Federntechnik
70	6	SaSy electromagnet	Magnetbau Schramme
71	6	SaSy anchor plate magnet	Magnetbau Schramme
72	12	SaSy slide bearing WSM 2022-15	igus
73	6	SaSy slide bearing WSM 1820-20	igus
74	6	SaSy bracket spring knee joint	Alu Boll, EN AW 2007, round rod 90 mm
75	6	SaSy bracket spring frame	Alu Boll, EN AW 2007, round rod 90 mm
76	12	SaSy slide bearing WSM 2023-08	igus
77	6	SaSy slide bearing WSM 2023-23	igus
78	3	Bracket cable gland	Alu Boll, EN AW 6082, eroded to outer contour
79	3	Baseplate cable grand hexapod strut	Stock item, Aluminium, flat bar 100 mm x 35 mm x 5 mm
80	1	Bracket accumulator	Alu Boll, EN AW 6060, rectangular tube 80 mm x 30 mm x 2 mm
81	2	Insert bracket accumulator	Alu Boll, EN AW 6082, flat bar 70 mm x 20 mm x 25 mm
82	2	Bracket accumulator stand	Alu Boll, EN AW 6082, flat bar 70 mm x 20 mm x 100 mm
83	1	Front bracket accumulator	Alu Boll, EN AW 6082, flat bar, 25 mm x 6 mm x 280 mm
84	1	Back bracket accumulator	Alu Boll, EN AW 6060, T profile, 60 mm x 60 mm x 6 mm
85	2	Bracket HV-box	Alu Boll, EN AW 6082, flat bar, 25 mm x 6 mm x 175 mm
86	6	SaSy bar	Alu Boll, EN AW 6060, rectangular tube 100 mm x 60 mm x 3 mm
87	6	SaSy bar strut	Alu Boll, EN AW 6060, rectangular tube 40 mm x 40 mm x 2 mm
88	12	SaSy bar elbow	Alu Boll, EN AW 6060, elbow 130 mm x 80 mm x 6 mm
89	6	SaSy upper left flange bar strut	Alu Boll, EN AW 6060, elbow 40 mm x 30 mm x 3 mm

Part Number	Qty.	Part name	Supplier, Material, Dimension
90	6	SaSy upper right flange bar strut	Alu Boll, EN AW 6060, elbow 40 mm x 30 mm x 3 mm
91	6	SaSy lower left flange bar strut	Alu Boll, EN AW 6060, elbow 35 mm x 30 mm x 3 mm
92	6	SaSy lower right flange bar strut	Alu Boll, EN AW 6060, elbow 35 mm x 30 mm x 3 mm
93	6	SaSy left elbow spring	Alu Boll, EN AW 6060, elbow 150 mm x 100 mm x 10 mm
94	30	SaSy sleeve M10	Alu Boll, EN AW 6060, round tube 20 mm x 5 mm
95	6	SaSy upper insert bar	Alu Boll, EN AW 6082, plate 54 mm x 94 mm x 20 mm
96	24	SaSy outer insert crossbeam	Alu Boll, EN AW 6082, plate 47 mm x 144 mm x 20 mm
97	12	SaSy inner insert crossbeam	Alu Boll, EN AW 6082, plate 50 mm x 144 mm x 20 mm
98	24	SaSy ribs elbow bar	Alu Boll, EN AW 6082, eroded to outer contour
99	12	SaSy ribs elbow spring	Alu Boll, EN AW 6082, eroded to outer contour
100	6	SaSy upper bolt	Geier, 1.4301, round rod 20 mm
101	6	SaSy lower bolt	Geier, 1.4301, round rod 22 mm
102	3	SaSy left cross brace	Geier, 1.4301, round tube 25 mm x 2 mm
103	6	SaSy upper baseplate cross brace	Geier, 1.4301, sheet metal 190 mm x 100 mm x 4 mm
104	6	SaSy lower baseplate cross brace	Geier, 1.4301, sheet metal 78 mm x 56 mm x 4 mm
105	6	SaSy sleeve M8 short	Alu Boll, EN AW 6060, round tube 20 mm x 5 mm
106	24	SaSy sleeve M8 long	Alu Boll, EN AW 6060, round tube 20 mm x 5 mm
107	12	SaSy sleeve M8 cross brace	Alu Boll, EN AW 6060, round tube 20 mm x 5 mm
108	6	SaSy adapter plate brake shoe	Alu Boll, EN AW 6082, eroded to outer contour
109	6	SaSy adapter piece brake shoe long	Alu Boll, EN AW 6082, eroded to outer contour
110	6	SaSy adapter piece brake shoe short	Alu Boll, EN AW 6082, eroded to outer contour
111	6	SaSy brake shoe	Bänfer
112	6	SaSy lower insert bar	Alu Boll, EN AW 6082, plate 54 mm x 94 mm x 20 mm
113	6	SaSy spacer upper bearing block	Alu Boll, EN AW 6082, eroded to outer contour
114	6	SaSy bracket magnet	Alu Boll, EN AW 2007, round rod 100 mm, length 162 mm
115	1	HV accumulator	Self-manufactured
116	1	HV-box	Stock item
117	6	Vertical clamping element	Stock item, Stahl, rectangular tube 100 mm x 60 mm x 3 mm
118	3	Crossbeam jack-up system	Stock item, Stahl, rectangular tube 120 mm x 60 mm x 3 mm
119	3	lower horizontal clamping element jack-up system	Stock item, Stahl, rectangular tube 100 mm x 60 mm x 3 mm
120	3	upper horizontal clamping element jack-up system	Stock item, Stahl, plate 110 mm x 100 mm x 20 mm

Part Number	Qty.	Part name	Supplier, Material, Dimension
121	3	Base insert clamping element jack-up system	Stock item, Stahl, plate 110 mm x 100 mm x 20 mm
122	3	Castor jack-up system	Rollentechnik
123	3	Screw connection castor jack-up system	Stock item, Stahl, plate 125 mm x 100 mm x 20 mm
124	3	SaSy right elbow spring	Alu Boll, EN AW 6060, elbow 150 mm x 100 mm x 10 mm
125	3	SaSy lower left flange bar strut bearing	Alu Boll, EN AW 6060, elbow 35 mm x 30 mm x 3 mm
126	3	SaSy lower right flange bar strut bearing	Alu Boll, EN AW 6060, elbow 35 mm x 30 mm x 3 mm
127	12	SaSy lower insert bar rail	Alu Boll, EN AW 6082, plate 54 mm x 94 mm x 20 mm
128	6	SaSy spacer bracket magnet	Alu Boll, EN AW 2007, round rod 100 mm, length 14,5 mm
129	12	SaSy upper sleeve M8 bar strut	Alu Boll, EN AW 6060, round tube 20 mm x 5 mm
130	1	SaSy spring compressor clamping plate magnet	Alu Boll, EN AW 7075, eroded to outer contour
131	1	SaSy spring compressor clamping plate knee lever	Alu Boll, EN AW 7075, eroded to outer contour
132	3	Baseplate cable grand frame	Stock item, Aluminium, flat bar 100 mm x 35 mm x 5 mm
133	6	SaSy adapter bump stop	Geier, EN AW 6060 T66, flat bar 60 mm x 25 mm
134	3	SaSy right cross brace	Geier, 1.4301, round tube 25 mm x 2 mm
135	6	SaSy counter-plate bump stop	Alu Boll
136	3	SaSy left bracket switch	Stock item, Aluminium, elbow 30 mm x 30 mm x 2 mm
137	3	SaSy right bracket switch	Stock item, Aluminium, elbow 30 mm x 30 mm x 2 mm
138	6	SaSy switch	Elektro Zimmermann
139	6	SaSy outer flange damper	Stock item, Stahl, flat bar 96 mm x 60 mm x 12 mm
140	6	SaSy damper	Stabilus
141	12	SaSy insert bar damper	Alu Boll, EN AW 6082, plate 54 mm x 94 mm x 20 mm
142	3	Bracket magnetic sensor	Stock item, Aluminium, flat bar 40 mm x 10 mm x 300 mm
143	2	Bracket LV-fuse box base bar	Stock item, Aluminium, flat bar 18 mm x 5 mm x 170 mm
144	4	Bracket LV-fuse box strut	Stock item, Aluminium, square bar 10 mm x 10 mm x 50 mm
145	1	Baseplate HV accumulator	Alu Boll, Aluminium, eroded to outer contour
146	6	SaSy bump stop	Gummi
147	12	SaSy vertical insert bar	Alu Boll, EN AW 6082, plate 94 mm x 60 mm x 20 mm
148	6	SaSy bracket anchor plate	Alu Boll, EN AW 6082
148	12	SaSy mandrel sleeve	Alu Boll, EN AW 6082
149	1	ADMA	GeneSys
150	1	Roadbox	IPG

Part Number	Qty.	Part name	Supplier, Material, Dimension
151	1	LV-fuse box	
152	4	LV accumulator	VARTA
152	1	GPS receiver	
152	1	DGPS antenna	
153	1	Wireless emergency stop receiver	

C.2 Preliminary Hazard List

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Steering unit	1.1	No or insufficient HV power supply	Demanded steering angle cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, HV energy cut is sudden and can hardly be detected prior to hazardous event, emergency braking possible, mitigation is possible	2	HV accumulator and safety-oriented BMS can lead to HV power cut	*2*	The DS trajectory must remain controllable in case of a HV power cut so that collisions with objects and subjects can be avoided
	1.2	No or insufficient LV power supply	The motor controller is unable to process its signals -> demanded steering angle cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, emergency braking possible, mitigation is possible	1	Standard LV accumulator and standard BMS make LV power cut more unlikely than HV power cut	*1*	The DS trajectory must remain controllable in case of a LV power cut so that collisions with objects and subjects can be avoided
	1.3.1	HV input power too high	Motor controller goes into safety shutdown -> demanded steering angle cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, mitigation is possible	2	HV accumulator cannot provide more than its maximum voltage, except when recuperation is in process.	*2*	The DS trajectory must remain controllable in case of a HV overvoltage so that collisions with objects and subjects can be avoided AND HV overvoltage because of recuperation must be avoided
	1.3.2		Motor controller fails to go into safety shutdown -> overvoltage in power electronics -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, mitigation is possible	1	The supplier developed its motor controller according to applicable standards and equipped the controller with overvoltage protection	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND HV overvoltage because of recuperation must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Steering unit	1.3.3	HV input power too high	Motor controller fails to go into safety shutdown -> overvoltage in power electronics -> short circuit and possibly fire hazard	Maintenance	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, mitigation is possible	1	The supplier developed its motor controller according to applicable standards and equipped the controller with overvoltage protection	*a*	HV overvoltage because of recuperation must be avoided
	1.4.1	LV input power too high	Motor controller goes into safety shutdown -> demanded steering angle cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*1*	The DS trajectory must remain controllable in case of a LV overvoltage so that collisions with objects and subjects can be avoided
	1.4.2		Motor controller fails to go into safety shutdown -> overvoltage in power electronics -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	1.5.1	Electric motor provides no/less/more torque than demanded	Incorrect torque leads to no/decreased/increased steering angle rate and therefore incorrect steering angle -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over steering is given, emergency braking is possible, mitigation is possible	1	Electric motor that is also used in light aircrafts, output voltage of motor controller translates directly to motor torque	*1*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Steering unit	1.5.2	Electric motor provides no/less/more torque than demanded	Incorrect torque leads to no/decreased/increased steering angle rate and therefore incorrect steering angle -> DS trajectory is uncontrollable	Maintenance, service engineer(s) standing close by electric motor	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled service engineer, control inputs to the DS can be checked before executing them, mitigation is possible	1	Electric motor that is also used in light aircrafts, output voltage of motor controller translates directly to motor torque	*a*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided
	1.6	Resolver delivers no electric motor speed signal	Motor controller is unable to control motor speed -> demanded steering angle cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over steering is given, emergency braking is possible, mitigation is possible	1	The supplier developed its resolver according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided
	1.7	Resolver delivers too low/high electric motor speed signal	Motor controller demand too high/low torque from electric motor -> too high/low steering angle -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over steering is given, emergency braking is possible, mitigation is possible	1	The supplier developed its resolver according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Steering unit	1.8.1	Temperature sensor delivers no/too low/high electric motor temperature signals	Motor controller reduces maximum electric motor torque or shuts electric motor down -> demanded steering angle cannot be provided -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only one temperature sensor fails limited control over steering is given, emergency braking possible, mitigation is possible	1	Electric motor (and temperature sensor) that is also used in light aircrafts	*1*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided
	1.8.2		Motor controller fails to reduce electric motor torque or to shut electric motor down -> overheating of electric motor -> possibly short circuit and/or fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Electric motor (and temperature sensor) that is also used in light aircrafts, motor controller developed according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	1.9.1	Motor controller provides no/too low/too high power to electric motor	No/too low/too high torque from electric motor -> demanded steering angle cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, detection possible by comparing the signals of all three steering motors, if only one motor controller fails limited control over steering is given, emergency braking possible, mitigation is possible	1	The supplier developed its motor controller according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning motor controller so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Steering unit	1.9.2	Motor controller provides no/too low/too high power to electric motor	Overvoltage in electric motor -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, maximum output voltage can be set in motor controller, mitigation is possible	1	The supplier developed its motor controller according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	1.10.1	Electric motor becomes too hot	Motor controller reduces maximum engine torque or shuts electric motor down -> demanded steering angle cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only electric motor fails limited control over steering is given, emergency braking possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, prototype electric motor (and temperature sensor) that is also used in light aircrafts, motor controller monitors temperatures	*1*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided
	1.10.2		Overheating of electric motor -> possibly short circuit and/or fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, prototype electric motor (and temperature sensor) that is also used in light aircrafts, motor controller monitors temperatures	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Steering unit	1.11.1	Motor controller becomes too hot	Motor controller goes into safety shutdown -> demanded steering angle cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only electric motor fails limited control over steering is given, emergency braking possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its motor controller according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning motor controller so that collisions with objects and subjects can be avoided
	1.11.2		Motor controller fails to go into safety shutdown -> overheating of motor controller -> possibly short circuit and/or fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its motor controller according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	1.12.1	Water ingress at electric motor	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at electric motor must be avoided
	1.12.2			Maintenance, service engineer working at the electric motor	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at electric motor must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Steering unit	1.12.3	Water ingress at electric motor	Electric motor is unable to operate -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	The DS trajectory must remain controllable in case of water ingress at the electric motor so that collisions with objects and subjects can be avoided
	1.13.1	Water ingress at motor controller	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at motor controller must be avoided
	1.13.2			Maintenance, service engineer working at the motor controller	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at motor controller must be avoided
	1.13.3		Motor controller is unable to operate -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	The DS trajectory must remain controllable in case of water ingress at the motor controller so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Steering unit	1.14	Motor controller provides no/incorrect/too late information to IPG Roadbox	IPG Roadbox is unable to calculate correct WMDS state -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	2	Skilled system operator, no direct control over motor controller, no mitigation possible	1	The supplier developed its motor controller according to applicable standards	*2*	The DS trajectory must remain controllable in case of a faulty data transmission from the motor controller to the IPG Roadbox so that collisions with objects and subjects can be avoided
Drive unit	2.1	No or insufficient HV energy supply	Demanded motor torque cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, HV energy cut is sudden and can hardly be detected prior to hazardous event, steering is possible, mitigation is possible	2	HV accumulator and safety-oriented BMS can lead to HV power cut	*2*	The DS trajectory must remain controllable in case of a HV power cut so that collisions with objects and subjects can be avoided
	2.2	No or insufficient LV energy supply	The motor controller is unable to process its signals -> demanded motor torque cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, HV energy cut is sudden and can hardly be detected prior to hazardous event, steering is possible, mitigation is possible	1	Standard LV accumulator and standard BMS make LV power cut more unlikely than HV power cut	*1*	The DS trajectory must remain controllable in case of a LV power cut so that collisions with objects and subjects can be avoided
	2.3.1	HV input voltage too high	Motor controller goes into safety shutdown -> demanded motor torque cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, mitigation is possible	2	HV accumulator cannot provide more than its maximum voltage, except when recuperation is in process.	*2*	The DS trajectory must remain controllable in case of a HV overvoltage so that collisions with objects and subjects can be avoided AND HV overvoltage because of recuperation must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Drive unit	2.3.2	HV input voltage too high	Motor controller fails to go into safety shutdown -> overvoltage in power electronics -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, mitigation is possible	1	The supplier developed its motor controller according to applicable standards and equipped the controller with overvoltage protection	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND HV overvoltage because of recuperation must be avoided
	2.3.3		Motor controller fails to go into safety shutdown -> overvoltage in power electronics -> short circuit and possibly fire hazard	Maintenance	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, mitigation is possible	1	The supplier developed its motor controller according to applicable standards and equipped the controller with overvoltage protection	*a*	HV overvoltage because of recuperation must be avoided
	2.4.1	LV input voltage too high	Motor controller goes into safety shutdown -> demanded motor torque cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*1*	The DS trajectory must remain controllable in case of a LV overvoltage so that collisions with objects and subjects can be avoided
	2.4.2		Motor controller fails to go into safety shutdown -> overvoltage in power electronics -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Drive unit	2.5.1	Electric motor provides no/less/more torque than demanded	Incorrect torque leads to no/decreased/increased wheel speeds and therefore incorrect velocity/acceleration and possibly yaw motion -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	Electric motor that is also used in light aircrafts, output voltage of motor controller translates directly to motor torque	*1*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided
	2.5.2			Maintenance, service engineer standing close by electric motor	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled service engineer, control inputs to the DS can be checked before executing them, mitigation is possible	1	Electric motor that is also used in light aircrafts, output voltage of motor controller translates directly to motor torque	*a*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided
	2.6	Resolver delivers no electric motor speed signal	Motor controller is unable to control motor speed -> demanded motor torque cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	The supplier developed its resolver according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided
	2.7	Resolver delivers too low/high electric motor speed signal	Motor controller demand too high/low torque from electric motor -> too high/low motor torque -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	The supplier developed its resolver according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Drive unit	2.8.1	Temperature sensor delivers no/too low/high electric motor temperature signals	Motor controller reduces maximum electric motor torque or shuts electric motor down -> demanded motor torque cannot be provided -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only one temperature sensor fails limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	Electric motor (and temperature sensor) that is also used in light aircrafts	*1*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided
	2.8.2		Motor controller fails to reduce electric motor torque or to shut electric motor down -> overheating of electric motor -> possibly short circuit and/or fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Electric motor (and temperature sensor) that is also used in light aircrafts, motor controller developed according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	2.9.1	Motor controller provides no/too low/too high voltage to electric motor	No/too low/too high torque from electric motor -> demanded motor torque cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, detection possible by comparing the signals of all three steering motors, if only one motor controller fails limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	The supplier developed its motor controller according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning motor controller so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Drive unit	2.9.2	Motor controller provides no/too low/too high voltage to electric motor	Overvoltage in electric motor -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, maximum output voltage can be set in motor controller, mitigation is possible	1	The supplier developed its motor controller according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	2.10.1	Electric motor becomes too hot	Motor controller reduces maximum engine torque or shuts electric motor down -> demanded motor torque cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only electric motor fails limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, prototype electric motor (and temperature sensor) that is also used in light aircrafts, motor controller monitors temperatures	*1*	The DS trajectory must remain controllable in case of a malfunctioning electric motor so that collisions with objects and subjects can be avoided
	2.10.2		Overheating of electric motor -> possibly short circuit and/or fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, prototype electric motor (and temperature sensor) that is also used in light aircrafts, motor controller monitors temperatures	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Drive unit	2.11.1	Motor controller becomes too hot	Motor controller goes into safety shutdown -> demanded motor torque cannot be provided -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only electric motor fails limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its motor controller according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning motor controller so that collisions with objects and subjects can be avoided
	2.11.2		Motor controller fails to go into safety shutdown -> overheating of motor controller -> possibly short circuit and/or fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its motor controller according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	2.12.1	Water ingress at electric motor	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at electric motor must be avoided
	2.12.2			Maintenance, service engineer working at the electric motor	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at electric motor must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Drive unit	2.12.3	Water ingress at electric motor	Electric motor is unable to operate -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	The DS trajectory must remain controllable in case of water ingress at the electric motor so that collisions with objects and subjects can be avoided
	2.13.1	Water ingress at motor controller	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at motor controller must be avoided
	2.13.2			Maintenance, service engineer working at the motor controller	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at motor controller must be avoided
	2.13.3		Motor controller is unable to operate -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	The DS trajectory must remain controllable in case of water ingress at the motor controller so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Drive unit	2.14	Motor controller provides no/incorrect/too late information to IPG Roadbox	IPG Roadbox is unable to calculate correct WMDS state -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	2	Skilled system operator, no direct control over motor controller, no mitigation possible	1	The supplier developed its motor controller according to applicable standards	*2*	The DS trajectory must remain controllable in case of a faulty data transmission from the motor controller to the IPG Roadbox so that collisions with objects and subjects can be avoided
Hexapod	3.1	No or insufficient HV power supply	Power electronics shut down -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	2	Skilled system operator, emergency shutdown and HV energy cut are sudden and can hardly be detected prior to hazardous event, no mitigation possible	2	HV accumulator and safety-oriented BMS can lead to HV power cut	*1*	Test person must remain accessible in case of HV power cut
	3.2.1	HV input power too high	Power electronics goes into safety shutdown -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, mitigation is possible	2	HV accumulator cannot provide more than its maximum voltage, except when recuperation is in process.	*a*	Test person must remain accessible in case of HV overvoltage AND HV overvoltage because of recuperation must be avoided
	3.2.2		Power electronics fail to go into safety shutdown -> overvoltage at power electronics -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, mitigation is possible	1	The supplier developed its power electronics according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND HV overvoltage because of recuperation must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Hexapod	3.3.1	Linear actuator provides no/less/more force than demanded	Motion of the linear actuators does not match the inverse kinematics model -> tension within hexapod may lead to fracture of actuator -> other actuators cannot support static and dynamic dome load -> instable or loose dome	Driving simulation with test person	2	Test person may be seriously injured or even killed	2	Regular application	2	Skilled system operator, no direct control over inverse kinematics model or voltage provided to actuators, no mitigation possible	1	The suppliers developed their actuators according to applicable standards	*1*	The test person must not be seriously injured or killed if the dome becomes loose or instable
	3.3.2			Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	2	Skilled service engineer/mechanic, no direct control over inverse kinematics model or voltage provided to actuators, no mitigation possible	1	The suppliers developed their actuators according to applicable standards	*1*	The service engineer(s) and/or mechanic(s) must not be seriously injured or killed if the dome becomes loose or instable
	3.4	Linear actuator's position sensor delivers no signal	Power electronics cannot control the linear actuator's position -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, safe hexapod position can be reached with open-loop control, mitigation is possible	1	The supplier developed its actuators and sensors according to applicable standards	*a*	Test person must remain accessible in case of a malfunctioning hexapod actuator

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Hexapod	3.5	Linear actuator's position sensor delivers too low/high signal	Power electronics demands too high/low actuator force -> motion of the linear actuators does not match the inverse kinematics model -> tension within hexapod may lead to fracture of actuator -> other actuators cannot support static and dynamic dome load -> instable or loose dome	Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	2	Skilled service engineer/mechanic, no direct control over inverse kinematics model or voltage provided to actuators, no mitigation possible	1	The supplier developed its actuators and sensors according to applicable standards	*1*	The service engineer(s) and/or mechanic(s) must not be seriously injured or killed if the dome becomes loose or instable
	3.6.1	Linear actuator's temperature sensor delivers no/too low/high signal	Power electronics reduce maximum actuator force or shuts actuator down -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, temperatures can be monitored and compared, mitigation possible	1	The supplier developed its actuators and sensors according to applicable standards	*a*	Test person must remain accessible in case of a malfunctioning hexapod actuator
	3.6.2		Power electronics fails to reduce maximum actuator force or to shut actuator down -> overheating of actuator -> possibly short circuit and fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored and compared, mitigation possible	1	The supplier developed its actuators and sensors according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Hexapod	3.7.1	Power electronics provide no/too low/too high power to linear actuator	No/too low/too high force from one linear actuator -> motion of the linear actuators does not match the inverse kinematics model -> tension within hexapod may lead to fracture of actuator -> other actuators cannot support static and dynamic dome load -> instable or loose dome	Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	2	Skilled service engineer/mechanic, no direct control over inverse kinematics model or voltage provided to actuators, no mitigation possible	1	The supplier developed its power electronics according to applicable standards	*1*	The service engineer(s) and/or mechanic(s) must not be seriously injured or killed if the dome becomes loose or instable
	3.7.2		Too high force from all linear actuators -> acceleration of the hexapod above demanded acceleration	Driving simulation with test person	1	Test person may be injured	2	Regular application	2	Skilled system operator, no direct control over actuators, no mitigation possible	1	The supplier developed its power electronics according to applicable standards	*a*	Malfunctioning power electronics must be avoided
	3.7.3		Overvoltage at linear actuator -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	2	Skilled system operator, no direct control over actuators, no mitigation possible	1	The supplier developed its power electronics according to applicable standards	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Hexapod	3.8.1	Linear actuator becomes too hot	Power electronics reduces maximum actuator force or shuts actuator down -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its actuators and sensors according to applicable standards	*a*	Test person must remain accessible in case of a malfunctioning hexapod actuator
	3.8.2		Power electronics fails to reduce maximum actuator force or to shut actuator down -> overheating of actuator -> possibly short circuit and fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its actuators and sensors according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	3.9.1	Power electronics become too hot	Power electronics goes into safety shutdown -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its power electronics according to applicable standards	*a*	Test person must remain accessible in case of a malfunctioning hexapod actuator

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Hexapod	3.9.2	Power electronics become too hot	Power electronics fails to go into safety shutdown -> overheating of power electronics -> possibly short circuit and/or fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its power electronics according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	3.10	The motion of one or more linear actuators, demanded by the power electronics, does not match the inverse kinematics model	Tension within hexapod may lead to fracture of actuator -> other actuators cannot support static and dynamic dome load -> instable or loose dome	Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	2	Skilled service engineer/mechanic, no direct control over actuators, no mitigation possible	1	The supplier developed its power electronics according to applicable standards	*1*	The service engineer(s) and/or mechanic(s) must not be seriously injured or killed if the dome becomes loose or instable
	3.11.1	Water ingress at linear actuator	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at hexapod actuator must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Hexapod	3.11.2	Water ingress at linear actuator	Short circuit and possibly fire hazard	Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Maintenance at hexapod	1	Skilled service engineer and mechanic, water ingress can be observed, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*1*	Water ingress at hexapod actuator must be avoided
	3.11.3			Emergency rescue	3	Test person and/or emergency personnel may be seriously injured or even killed	1	Rare emergency use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*1*	Water ingress at hexapod actuator must be avoided
	3.11.4		Linear actuator is unable to operate -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*a*	Test person must remain accessible in case of a malfunctioning hexapod actuator
	3.12.1	Water ingress at power electronics	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at hexapod power electronics must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Hexapod	3.12.2	Water ingress at power electronics	Power electronics is unable to operate -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*a*	Water ingress at hexapod power electronics must be avoided
	3.13	Power electronics provide no/incorrect/too late information to IPG Roadbox	IPG Roadbox is unable to calculate correct WMDS state -> hexapod motion is uncontrollable	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	2	Skilled system operator, no direct control over power electronics, no mitigation possible	1	The supplier developed its power electronics according to applicable standards	*a*	Test person must remain accessible in case of a faulty data transmission from the power electronics to the IPG Roadbox
Mock-up	4.1.1	No or insufficient power supply	Test person is unable to give control inputs	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	2	Skilled system operator, energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard BMS make LV power cut more unlikely than HV power cut	*a*	Test person must be able to give control inputs
	4.1.2		Test person is unable to communicate with system operator and vice versa	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	2	Skilled system operator, energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard BMS make LV power cut more unlikely than HV power cut	*a*	Test person must be able to communicate with system operator and vice versa

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.1.3	No or insufficient power supply	Test person cannot receive system feedback through visual, auditory, and tactile channels	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	2	Skilled system operator, energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard BMS make LV power cut more unlikely than HV power cut	*a*	Test person must receive visual, auditory, and tactile feedback
	4.1.4		Test person cannot receive system feedback through visual, auditory, and tactile channels -> test person gets motion sick and throws up onto E/E/PE element -> short circuit and possible fire hazard -> test person must be rescued	Driving simulation with test person, dynamic driving situation	3	Test person and/or emergency personnel may be seriously injured or even killed	1	Regular use case, rare event	1	Skilled system operator, test person can be monitored and driving simulation can be aborted prior to critical event, mitigation is possible	1	Standard LV accumulator and standard BMS make LV power cut more unlikely than HV power cut	*a*	Test person must receive visual, auditory, and tactile feedback
	4.1.5		System operator is unable to monitor test person	Driving simulation or emergency rescue with unclear situation for test person, test person might unbuckle and/or move within move	2	Test person may be seriously injured or even killed	1	Regular use case, rare event	2	Skilled system operator, energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard BMS make LV power cut more unlikely than HV power cut	*a*	System operator must be able to monitor test person

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.1.6	No or insufficient power supply	System operator is unable to monitor test person	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	2	Skilled system operator, energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard BMS make LV power cut more unlikely than HV power cut	*a*	System operator must be able to monitor test person
	4.1.7		Air conditioning is unable to operate	Driving simulation with test person, extremely cold/hot environmental conditions	2	Frostbite/Heat stroke	1	Regular use case, rare event	1	Unskilled test person, when dome gets too cold/hot test person can leave DS, mitigation is possible	1	Standard LV accumulator and standard BMS make LV power cut more unlikely than HV power cut, extreme temperatures excluded from environmental conditions	*a*	Air conditioning must be available at all times
	4.2.1	Input power too high	Control elements go into safety shutdown -> test person cannot give control inputs	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*	Test person must be able to give control inputs
	4.2.2		Representation elements go into safety shutdown -> test person cannot receive system feedback through visual, auditory, and tactile channels	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*	Test person must receive visual, auditory, and tactile feedback

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.2.3	Input power too high	Communication system goes into safety shutdown -> test person is unable to communicate with system operator and vice versa	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	1	Regular use case, rare event	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*	Test person must be able to communicate with system operator and vice versa
	4.2.4		Surveillance system goes into safety shutdown -> system operator is unable to monitor test person	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	1	Regular use case, rare event	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*	System operator must be able to monitor test person
	4.2.5		Air conditioning goes into safety shutdown -> air conditioning is unable to operate	Driving simulation with test person, extremely cold/hot environmental conditions	2	Frostbite/Heat stroke	1	Regular use case, rare event	1	Unskilled test person, when dome gets too cold/hot test person can leave DS, mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage, extreme temperatures excluded from environmental conditions	*a*	Air conditioning must be available at all times

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.2.6	Input power too high	Any of the subsystem's elements fails to go into safety shutdown -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage, suppliers of subsystem's elements developed their components according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	4.3	Gear selection is not/not properly sensed	No/wrong gear selection is forwarded to WMDS dynamics control subsystem -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its gear selection system according to applicable standards	*a*	Gear selection must be correctly sensed at all times
	4.4	Steering wheel angle is not/not properly sensed	No/wrong steering wheel angle is forwarded to WMDS dynamics control subsystem -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its steering wheel according to applicable standards	*a*	Steering wheel angle must be correctly sensed at all times
	4.5	Clutch pedal position is not/not properly sensed	No/wrong clutch pedal position is forwarded to WMDS dynamics control subsystem -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its pedal assembly according to applicable standards	*a*	Clutch pedal position must be correctly sensed at all times

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.6	Brake pedal position is not/not properly sensed	No/wrong brake pedal position is forwarded to WMDS dynamics control subsystem -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its pedal assembly according to applicable standards	*a*	Brake pedal position must be correctly sensed at all times
	4.7	Accelerator pedal position is not/not properly sensed	No/wrong accelerator pedal position is forwarded to WMDS dynamics control subsystem -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its pedal assembly according to applicable standards	*a*	Accelerator pedal position must be correctly sensed at all times
	4.8	Steering wheel force feedback actuator gives no/too low/too high feedback force	False cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Unskilled test person, when false cues are represented test person can communicate with system operator and abort driving simulation, mitigation is possible	1	Supplier developed its steering wheel according to applicable standards	*a*	Correct steering wheel force feedback must be provided at all times
	4.9	Brake pedal's ABS shaker gives no/too low/too high feedback force	False cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Unskilled test person, when false cues are represented test person can communicate with system operator and abort driving simulation, mitigation is possible	1	Supplier developed its pedal assembly according to applicable standards	*a*	Correct ABS shaker feedback must be provided at all times

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.10	Sound system gives no/wrong/too early/too late auditory feedback	False cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Unskilled test person, when false cues are represented test person can communicate with system operator and abort driving simulation, mitigation is possible	1	Supplier developed its sound system according to applicable standards	*a*	Correct acoustical cues must be provided at all times
	4.11	Visual representation system gives no/wrong/too early/too late visual feedback	False cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Unskilled test person, when false cues are represented test person can communicate with system operator and abort driving simulation, mitigation is possible	1	Supplier developed its visual representation system according to applicable standards	*a*	Correct visual cues must be provided at all times
	4.12	Air conditioning is set at too high/low air temperature	Temperature within dome is too low/high -> health hazard to test person	Driving simulation with test person	2	Frostbite/Heat stroke	2	Regular application	1	Unskilled test person, when dome gets too cold/hot test person can communicate with system operator and abort driving simulation and leave DS, mitigation is possible	1	Skilled system operator sets temperature, supplier developed its air conditioning according to applicable standards	*a*	Air conditioning must be available at all times
	4.13.1	Any of the representation elements becomes too hot	Representation element goes into safety shutdown -> test person cannot receive system feedback through visual, auditory, or tactile channels	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the suppliers developed their representation elements according to applicable standards	*a*	Correct visual, acoustical and tactile cues must be provided at all times

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.13.2	Any of the representation elements becomes too hot	Representation element fails to go into safety shutdown -> possibly short circuit and fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its power electronics according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	4.14.1	Any of the control elements becomes too hot	Control element goes into safety shutdown -> test person cannot give control inputs	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, temperatures and test person's control input and behaviour can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the suppliers developed their control input elements according to applicable standards	*a*	Test person's inputs must be correctly sensed at all times
	4.14.2		Control element fails to go into safety shutdown -> possibly short circuit and fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the suppliers developed their control input elements according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.15.1	Communication system becomes too hot	Communication system goes into safety shutdown -> test person is unable to communicate with system operator and vice versa	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its communication system according to applicable standards	*a*	Test person must be able to communicate with system operator and vice versa
	4.15.2		Communication system fails to go into safety shutdown -> possibly short circuit and fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its communication system according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	4.16.1	Surveillance system becomes too hot	Surveillance system goes into safety shutdown -> system operator is unable to monitor test person	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	1	Skilled system operator, test person can communicate with system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its surveillance system according to applicable standards	*a*	System operator must be able to monitor test person

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.16.2	Surveillance system becomes too hot	Surveillance system fails to go into safety shutdown -> possibly short circuit and fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its surveillance system according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	4.17.1	Air conditioning system becomes too hot	Air conditioning goes into safety shutdown -> air conditioning is unable to operate	Driving simulation with test person, extremely cold/hot environmental conditions	2	Frost-bite/Heat stroke	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its air conditioning according to applicable standards	*a*	Air conditioning must be available at all times
	4.17.2		Air conditioning fails to go into safety shutdown -> possibly short circuit and fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its air conditioning according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.18.1	Water ingress at visual representation system	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at the visual representation system must be avoided
	4.18.2		Visual representation system is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*a*	Correct visual cues must be provided at all times AND water ingress at the visual representation system must be avoided
	4.19.1	Water ingress at sound system	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at the sound system must be avoided
	4.19.2		Sound system is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*a*	Correct acoustical cues must be provided at all times AND water ingress at the sound system must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.20.1	Water ingress at steering wheel	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at the steering wheel must be avoided
	4.20.2		Steering wheel force feedback actuator is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*a*	Correct steering wheel force feedback must be provided at all times AND water ingress at the steering wheel must be avoided
	4.20.3		Steering wheel angle sensor is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*a*	Steering wheel angle must be correctly sensed at all times AND water ingress at the steering wheel must be avoided
	4.21.1	Water ingress at pedals	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at the pedals must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.21.2	Water ingress at pedals	Brake pedal ABS shaker is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*a*	Correct ABS shaker feedback must be provided at all times AND water ingress at the pedals must be avoided
	4.21.3		Brake and/or clutch and/or accelerator pedal sensor is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*a*	Brake/Accelerator/Clutch pedal position must be correctly sensed at all times AND water ingress at the pedals must be avoided
	4.22.1	Water ingress at communication system	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at the pedals must be avoided
	4.22.2		Communication system is unable to operate -> test person cannot communicate with system operator and vice versa	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*1*	Test person must be able to communicate with system operator and vice versa in case of water ingress at the communication system AND water ingress at the communication system must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.23.1	Water ingress at surveillance system	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at the pedals must be avoided
	4.23.2		Surveillance system is unable to operate -> system operator cannot monitor test person	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*a*	System operator must be able to monitor test person AND water ingress at the surveillance system must be avoided
	4.24.1	Water ingress at air conditioning	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at the pedals must be avoided
	4.24.2		Air conditioning is unable to operate -> health hazard to test person	Driving simulation with test person, extremely cold/hot environmental conditions	2	Frost-bite/Heat stroke	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, temperatures can be monitored, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*1*	Air conditioning must be available at all times AND water ingress at the air conditioning system must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Mock-up	4.25	Communication system does not/other than/too late forward the test person's input to external command device's communication system	System operator cannot/too late react to the test person's input	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	1	Skilled system operator, test person can be monitored, mitigation is possible	2	Wireless data transmission, supplier developed its communication system according to applicable standards	*a*	Test person must be able to communicate with system operator and vice versa in case of a faulty data transmission from the mock-up's to the external command device's communication system
	4.26	Surveillance system does not/other than/too late forward its information to the external command device's communication system	System operator cannot/too late react to the test person's behaviour/condition	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	1	Skilled system operator, test person can communicate with system operator, mitigation is possible	2	Wireless data transmission, supplier developed its surveillance system according to applicable standards	*a*	System operator must be able to monitor test person in case of a faulty data transmission from the surveillance system to the external command device
	4.27	Driver input not/incorrectly/too late forwarded to IPG Roadbox	False cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its components according to applicable standards	*a*	Test person's inputs must be correctly forwarded to the IPG Roadbox

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
External command device	5.1.1	No or insufficient power supply	System operator is unable to give control inputs -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace, MCA fails	3	Test person and/or bystanders and/or system operator may be injured and/or killed	1	Regular application, rare event	2	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Power cut from stationary power socket very unlikely	*1*	The DS trajectory must remain controllable in case of a stationary power cut so that collisions with objects and subjects can be avoided
	5.1.2			Manual drive, maximum manually adjustable driving velocity	3	Test person and/or bystanders and/or system operator may be injured and/or killed	1	Rare use case	2	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Power cut from stationary power socket very unlikely	*1*	The DS trajectory must remain controllable in case of a stationary power cut so that collisions with objects and subjects can be avoided
	5.1.3		External command device is unable to operate -> communication with and surveillance of test person impossible	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	1	Regular application, rare event	2	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Power cut from stationary power socket very unlikely	*a*	Test person must be able to communicate with system operator and vice versa in case of a stationary power cut
	5.2.1	Input power too high	External command device goes into safety shutdown -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace, MCA fails	3	Test person and/or bystanders and/or system operator may be injured and/or killed	1	Regular application, rare event	1	Skilled system operator, overvoltage in stationary power supply only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	Overvoltage stationary power socket very unlikely	*a*	The DS trajectory must remain controllable in case of a stationary power overvoltage so that collisions with objects and subjects can be avoided AND stationary power overvoltage must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
External command device	5.2.2	Input power too high	External command device fails to go into safety shutdown -> short circuit and possibly fire hazard	Driving simulation, system operator must be rescued	3	System operator(s) and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, overvoltage in stationary power supply only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	Overvoltage stationary power socket very unlikely	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND stationary power overvoltage must be avoided
	5.2.3			Maintenance	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled system operator, overvoltage in stationary power supply only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	Overvoltage stationary power socket very unlikely	*a*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND stationary power overvoltage must be avoided
	5.3.1	Water ingress at external command device	Short circuit and possibly fire hazard	Driving simulation, system operator must be rescued	3	System operator(s) and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at the external command device must be avoided
	5.3.2		External command device is unable to operate -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace, MCA fails	3	Test person and/or bystanders and/or system operator may be injured and/or killed	1	Regular application, rare event	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*1*	The DS trajectory must remain controllable in case of water ingress at the external command device AND water ingress at the external command device must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
External command device	5.3.3	Water ingress at external command device	External command device is unable to operate -> communication with and surveillance of test person impossible	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	1	Regular application, rare event	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*a*	Test person must be able to communicate with system operator and vice versa AND water ingress at the external command device must be avoided
	5.4.1	External command device becomes too hot	External command device goes into safety shutdown -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace, MCA fails	3	Test person and/or bystanders and/or system operator may be injured and/or killed	1	Regular application, rare event	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its external command device according to applicable standards	*a*	The DS trajectory must remain controllable in case of a malfunctioning external command device
	5.4.2		External command device fails to go into safety shutdown -> possibly short circuit and/or fire hazard	Driving simulation, system operator must be rescued	3	System operator(s) and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its external command device according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
External command device	5.5	Command inputs are not/incorrectly/too late forwarded to the WMDS dynamics control subsystem	System operator has no/wrong/delayed influence on DS trajectory	Driving simulation with test person, high velocity, close to boundary of DS workspace, MCA fails	3	Test person and/or bystanders and/or system operator may be injured and/or killed	1	Regular application, rare event	2	Skilled system operator, no mitigation possible	2	Wireless data transmission, supplier developed its external command device according to applicable standards	*2*	The DS trajectory must remain controllable in case of a faulty data transmission from the external command device to the WMDS dynamics control subsystem AND wireless data transmission must not fail
	5.6	Communication system does not/other than/too late forward the system operator's input to the mock-up E/E/PE subsystem's communication system	Test person cannot/too late react to the system operator's input	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	2	Regular applications	2	Unskilled test person, no communication possible, mitigation is hardly possible	2	Wireless data transmission, supplier developed its communication system according to applicable standards	*2*	Test person must be able to communicate with system operator and vice versa in case of a faulty data transmission from the external command device to the WMDS dynamics control subsystem AND wireless data transmission must not fail
WMDS dynamics ctrl	6.1	No or insufficient LV power supply	DS trajectory cannot be calculated -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	2	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard BMS make LV power cut more unlikely than HV power cut	*2*	The DS trajectory must remain controllable in case of a LV power cut so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
WMDS dynamics control	6.2.1	LV input power too high	IPG Roadbox goes into safety shutdown -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*1*	The DS trajectory must remain controllable in case of a LV power overvoltage so that collisions with objects and subjects can be avoided
	6.2.2		ADMA G-3 goes into safety shutdown -> closeloop control not possible, possibly dangerous trajectory	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), emergency braking is possible, mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*1*	The DS trajectory must remain controllable in case of a LV power overvoltage so that collisions with objects and subjects can be avoided
	6.2.3		IPG Roadbox and/or ADMA G-3 fails to go into safety shutdown -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	6.4.1	Water ingress at IPG Roadbox	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at the IPG Roadbox must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
WMDS dynamics control	6.4.2	Water ingress at IPG Roadbox	IPG Roadbox is unable to operate -> DS trajectory not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	The DS trajectory must remain controllable in case of water ingress at the IPG Roadbox so that collisions with objects and subjects can be avoided AND water ingress at the IPG Roadbox must be avoided
	6.5.1	Water ingress at ADMA G-3	Short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at the ADMA G-3 must be avoided
	6.5.2		ADMA-G3 is unable to operate -> position/motion of DS unclear -> DS trajectory not controllable in closed-loop control, possibly dangerous trajectory	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, open-loop control still possible, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	The DS trajectory must remain controllable in case of water ingress at the ADMA G-3 so that collisions with objects and subjects can be avoided AND water ingress at the ADMA G-3 must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
WMDS dynamics control	6.6.1	IPG Roadbox becomes too hot	IPG Roadbox goes into safety shutdown -> DS trajectory is uncontrollable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its Roadbox according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning IPG Roadbox so that collisions with objects and subjects can be avoided
	6.6.2		IPG Roadbox fails to go into safety shutdown -> possibly short circuit and/or fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its Roadbox according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	6.7.1	ADMA G-3 becomes too hot	ADMA G-3 goes into safety shutdown -> DS trajectory is uncontrollable in closed-loop control, possibly dangerous trajectory	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, open-loop control still possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its ADMA G-3 according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning ADMA G-3 so that collisions with objects and subjects can be avoided
	6.7.2		ADMA G-3 fails to go into safety shutdown -> possibly short circuit and/or fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, open-loop control still possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its ADMA G-3 according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
WMDS dynamics control	6.8	ADMA G-3 signals are not/incorrectly/too late forwarded to IPG Roadbox	Position/motion of DS unclear -> DS trajectory not controllable in closed-loop control, possibly dangerous trajectory	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, open-loop control still possible, emergency braking possible, mitigation is possible	1	Supplier developed its ADMA G-3 according to applicable standards	*1*	The DS trajectory must remain controllable in case of a faulty data transmission from ADMA G-3 to IPG Roadbox so that collisions with objects and subjects can be avoided
	6.9	IPG Roadbox signals are not/incorrectly/too late forwarded to steering unit subsystem	Incorrect steering angle is provided -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, emergency braking possible, no mitigation possible	3	Supplier developed its IPG Roadbox according to applicable standards, self-programmed dynamics control	*3*	The DS trajectory must remain controllable in case of a faulty data transmission from the IPG Roadbox to the steering unit subsystem so that collisions with objects and subjects can be avoided
	6.10	IPG Roadbox signals are not/incorrectly/too late forwarded to drive unit subsystem	Maximum wheel hub torque is provided -> DS trajectory is not controllable, steering impossible	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	2	Skilled system operator, no mitigation possible	3	Supplier developed its IPG Roadbox according to applicable standards, self-programmed dynamics control	*4*	The DS trajectory must remain controllable in case of a faulty data transmission from the IPG Roadbox to the drive unit subsystem so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
WMDS dynamics control	6.11	IPG Roadbox signals are not/incorrectly/too late forwarded to hexapod subsystem	Incorrect linear actuator force is provided -> false cues are generated and/or motion of the linear actuators does not match the inverse kinematics model -> tension within hexapod may lead to fracture of actuator -> other actuators cannot support static and dynamic dome load -> instable or loose dome	Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	2	Skilled system operator, no mitigation possible	3	Supplier developed its IPG Roadbox according to applicable standards, self-programmed dynamics control	*3*	The DS trajectory must remain controllable in case of a faulty data transmission from the IPG Roadbox to the hexapod subsystem so that collisions with objects and subjects can be avoided
	6.12	IPG Roadbox signals are not/incorrectly/too late forwarded to mock-up subsystem	Test person cannot receive system feedback through visual, auditory, and tactile channels	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	2	Skilled system operator, no mitigation possible	3	Supplier developed its IPG Roadbox according to applicable standards, self-programmed dynamics control	*2*	The DS trajectory must remain controllable in case of a faulty data transmission from the IPG Roadbox to the mock-up subsystem so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
WMDS dynamics control	6.13	IPG Roadbox signals are not/incorrectly/too late forwarded to external command device subsystem	System operator is unclear about the DS' driving state	Driving simulation with test person, high velocity, close to boundary of DS workspace, MCA fails	3	Test person and/or bystanders and/or system operator may be injured and/or killed	1	Regular application, rare event	2	Skilled system operator, no mitigation possible	3	Wireless data transmission, supplier developed its IPG Roadbox according to applicable standards, self-programmed dynamics control	*3*	The DS trajectory must remain controllable in case of a faulty data transmission from the IPG Roadbox to the external command device subsystem so that collisions with objects and subjects can be avoided
	6.14	ADMA G-3 position and/or motion are not/incorrectly measured	Position/motion of DS unclear -> DS trajectory not controllable in closed-loop control, possibly dangerous trajectory	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, open-loop control still possible, emergency braking possible, mitigation is possible	2	sensor noise, sensor drift, GPS is blind	*2*	The DS trajectory must remain controllable in case of faulty position and/or motion ADMA G-3 measurements so that collisions with objects and subjects can be avoided
Power supply	7.1	Traction battery's management system cuts power supply	Steering unit, drive unit, and hexapod E/E/PE subsystems cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	2	Skilled system operator, no direct control over BMS, no mitigation possible	2	HV accumulator and safety-oriented BMS can lead to HV power cut	*3*	The DS trajectory must remain controllable in case of a HV power cut so that collisions with objects and subjects can be avoided
	7.2.1	Overvoltage from traction battery	Steering unit, drive unit, and hexapod E/E/PE subsystems cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	2	Skilled system operator, no direct control over BMS, no mitigation possible	1	HV accumulator cannot provide more than its maximum voltage	*2*	The DS trajectory must remain controllable in case of a HV overvoltage so that collisions with objects and subjects can be avoided AND HV overvoltage because of recuperation must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Power supply	7.2.2	Overvoltage from traction battery	Short circuit and possibly fire hazard at steering unit, drive unit, and hexapod E/E/PE subsystems	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	2	Skilled system operator, no direct control over BMS, no mitigation possible	1	HV accumulator cannot provide more than its maximum voltage	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND HV overvoltage because of recuperation must be avoided
	7.3.1	Overvoltage from auxiliary battery	Steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its maximum voltage	*1*	The DS trajectory must remain controllable in case of a LV overvoltage so that collisions with objects and subjects can be avoided
	7.3.2		Short circuit and possibly fire hazard at steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its maximum voltage	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	7.4.1	Overvoltage from AC/DC converter	Mock-up E/E/PE subsystem cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	2	Skilled system operator, no direct control over AC/DC converter, no mitigation possible	1	LV accumulator cannot provide more than its maximum voltage, supplier developed its AC/DC converter according to applicable standards	*2*	The DS trajectory must remain controllable in case of a AC/DC converter overvoltage so that collisions with objects and subjects can be avoided AND AC/DC converter overvoltage must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Power supply	7.4.2	Overvoltage from AC/DC converter	Short circuit and possibly fire hazard at mock-up E/E/PE subsystem	Driving simulation with test person, system operator(s) must be rescued	3	System operator(s) and/or emergency personnel may be seriously injured or even killed	2	Regular application	2	Skilled system operator, no direct control over AC/DC converter, no mitigation possible	1	LV accumulator cannot provide more than its maximum voltage, supplier developed its AC/DC converter according to applicable standards	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND AC/DC converter overvoltage must be avoided
	7.5.1	Overvoltage from stationary power connection	External command device E/E/PE subsystem cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace, MCA fails	3	Test person and/or bystanders and/or system operator may be injured and/or killed	1	Regular application, rare event	1	Skilled system operator, overvoltage in stationary power supply only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	Overvoltage from power socket very unlikely	*a*	The DS trajectory must remain controllable in case of a stationary power connector overvoltage so that collisions with objects and subjects can be avoided
	7.5.2		Short circuit and possibly fire hazard at external command device E/E/PE subsystem	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, overvoltage in stationary power supply only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	Overvoltage from power socket very unlikely	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Power supply	7.6.1	Overvoltage from steering unit/drive unit E/E/PE subsystem when recuperating	Traction battery goes into safety shutdown -> steering unit, drive unit, and hexapod E/E/PE subsystems cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, recuperation can be avoided, mitigation is possible	3	Recuperation power is above maximum input power to traction battery, no conventional brakes	*3*	The DS trajectory must remain controllable in case of an overvoltage from the steering/drive unit subsystem (during recuperation) so that collisions with objects and subjects can be avoided AND overvoltage because of recuperation must be avoided
	7.6.2		Traction battery fails to go into safety shutdown -> short circuit and possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, recuperation can be avoided, mitigation is possible	3	Recuperation power is above maximum input power to traction battery, no conventional brakes	*3*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND overvoltage because of recuperation must be avoided
	7.7.1	Water ingress at traction battery	Steering unit, drive unit, and hexapod E/E/PE subsystems cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	HV accumulator and safety-oriented BMS can lead to HV power cut	*2*	The DS trajectory must remain controllable in case water ingress at traction battery so that collisions with objects and subjects can be avoided AND water ingress at traction battery must be avoided
	7.7.2		Short circuit and possibly fire hazard at steering unit, drive unit, and hexapod E/E/PE subsystems	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at traction battery must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Power supply	7.8.1	Water ingress at auxiliary battery	Steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	The DS trajectory must remain controllable in case water ingress at auxiliary battery so that collisions with objects and subjects can be avoided AND water ingress at auxiliary battery must be avoided
	7.8.2		Short circuit and possibly fire hazard at steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at auxiliary battery must be avoided
	7.9.1	Water ingress at AC/DC converter	Mock-up E/E/PE subsystem cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	The DS trajectory must remain controllable in case water ingress at AC/DC converter so that collisions with objects and subjects can be avoided AND water ingress at AC/DC converter must be avoided
	7.9.2		Short circuit and possibly fire hazard at mock-up E/E/PE subsystem	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at AC/DC converter must be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Power supply	7.10.1	Water ingress at stationary power connection	WMDS dynamics control E/E/PE subsystem cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace, MCA fails	3	Test person and/or bystanders and/or system operator may be injured and/or killed	1	Regular application, rare event	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*1*	The DS trajectory must remain controllable in case water ingress at stationary power connector so that collisions with objects and subjects can be avoided AND water ingress at stationary power connector must be avoided
	7.10.2		Short circuit and possibly fire hazard at WMDS dynamics control E/E/PE subsystem	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	2	Environmental conditions exclude high humidity and water, liquid could be brought into the system by users (e.g. for drinking)	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND water ingress at stationary power connector must be avoided
	7.11.1	Traction battery becomes too hot	Traction battery goes into safety shutdown -> steering unit, drive unit, and hexapod E/E/PE subsystems cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its traction battery and BMS according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning traction battery so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Power supply	7.11.2	Traction battery becomes too hot	Traction battery fails to go into safety shutdown -> Short circuit and possibly fire hazard at steering unit, drive unit, and hexapod E/E/PE subsystems	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its traction battery and BMS according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	7.12	Auxiliary battery becomes too hot	Auxiliary battery fails to go into safety shutdown -> short circuit and possibly fire hazard at steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	2	Skilled system operator, temperatures cannot be monitored (no sensors), no mitigation possible	1	Extreme heat excluded from environmental conditions, the supplier developed its auxiliary battery and BMS according to applicable standards	*2*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock AND auxiliary battery's temperature must be monitored
	7.13.1	AC/DC converter becomes too hot	AC/DC converter goes into safety shutdown -> mock-up E/E/PE subsystem cannot operate -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its AC/DC converter according to applicable standards	*1*	The DS trajectory must remain controllable in case of a malfunctioning AC/DC converter so that collisions with objects and subjects can be avoided

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Power supply	7.13.2	AC/DC converter becomes too hot	AC/DC converter fails to go into safety shutdown -> short circuit and possibly fire hazard at mock-up E/E/PE subsystem	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its AC/DC converter according to applicable standards	*1*	Continuous short circuit must be avoided so that during a rescue other subjects could get an electric shock
	7.14	Traction battery's SOC is not/incorrectly/too late transmitted to WMDS dynamics control system	System operator is unaware of traction battery's SOC -> WMDS may run out of HV power -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	2	Skilled system operator, no mitigation is possible	1	Supplier developed its BMS according to applicable standards	*2*	The DS trajectory must remain controllable in case of a faulty traction battery's SOC signal to the WMDS dynamics control system so that collisions with objects and subjects can be avoided
	7.15	Auxiliary battery's SOC is not/incorrectly/too late transmitted to WMDS dynamics control system	System operator is unaware of auxiliary battery's SOC -> WMDS may run out of LV power -> DS trajectory is not controllable	Driving simulation with test person, high velocity, close to boundary of DS workspace	3	Test person and/or bystanders and/or system operator may be injured and/or killed	2	Regular application	2	Skilled system operator, no mitigation is possible	1	Supplier developed its BMS according to applicable standards	*2*	The DS trajectory must remain controllable in case of a faulty auxiliary battery's SOC signal to the WMDS dynamics control system so that collisions with objects and subjects can be avoided

C.3 Revised Hazard List

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Steering unit	1.1	No or insufficient HV power supply	Safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, HV energy cut is sudden and can hardly be detected prior to hazardous event, emergency braking possible, mitigation is possible	1	HV accumulator and safety-oriented battery management system with high availability	*a*
	1.2	No or insufficient LV power supply	Safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, emergency braking possible, mitigation is possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*
	1.3.1	HV input power too high	Motor controller goes into safety shutdown -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, diodes and fuses avoid overvoltage, mitigation is possible	2	HV accumulator cannot provide more than its maximum voltage, except when recuperation is in process.	*a*
	1.3.2		Motor controller fails to go into safety shutdown -> overvoltage in power electronics -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, diodes and fuses avoid overvoltage, mitigation is possible	1	The supplier developed its motor controller according to applicable standards and equipped the controller with overvoltage protection	*a*
	1.3.3			Maintenance	1	Service engineer or mechanic may receive only minor injuries	1	Rare use case	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, diodes and fuses avoid overvoltage, mitigation is possible	1	The supplier developed its motor controller according to applicable standards and equipped the controller with overvoltage protection	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Steering unit	1.4.1	LV input power too high	Motor controller goes into safety shutdown -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by system operator (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*
	1.4.2		Motor controller fails to go into safety shutdown -> overvoltage in power electronics -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by system operator (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*
	1.5.1	Electric motor provides no/less/more torque than demanded	Incorrect torque leads to no/decreased/increased steering angle rate and therefore incorrect steering angle -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over steering is given, emergency braking is possible, mitigation is possible	1	Electric motor that is also used in light aircrafts, output voltage of motor controller translates directly to motor torque	*a*
	1.5.2			Maintenance, service engineer(s) standing close by electric motor	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled service engineer, control inputs to the DS can be checked before executing them, mitigation is possible	1	Electric motor that is also used in light aircrafts, output voltage of motor controller translates directly to motor torque	*a*
	1.6	Resolver delivers no electric motor speed signal	Motor controller is unable to control motor speed -> demanded steering angle cannot be provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over steering is given, emergency braking is possible, mitigation is possible	1	The supplier developed its resolver according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Steering unit	1.7	Resolver delivers too low/high electric motor speed signal	Motor controller demand too high/low torque from electric motor -> too high/low steering angle -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over steering is given, emergency braking is possible, mitigation is possible	1	The supplier developed its resolver according to applicable standards	*a*
	1.8.1	Temperature sensor delivers no/too low/high electric motor temperature signals	Motor controller reduces maximum electric motor torque or shuts electric motor down -> demanded steering angle cannot be provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only one temperature sensor fails limited control over steering is given, emergency braking possible, mitigation is possible	1	Electric motor (and temperature sensor) that is also used in light aircrafts	*a*
	1.8.2		Motor controller fails to reduce electric motor torque or to shut electric motor down -> overheating of electric motor -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Electric motor (and temperature sensor) that is also used in light aircrafts, motor controller developed according to applicable standards	*a*
	1.9.1	Motor controller provides no/too low/too high power to electric motor	No/too low/too high torque from electric motor -> demanded steering angle cannot be provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, detection possible by comparing the signals of all three steering motors, if only one motor controller fails limited control over steering is given, emergency braking possible, mitigation is possible	1	The supplier developed its motor controller according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Steering unit	1.9.2	Motor controller provides no/too low/too high power to electric motor	Overvoltage in electric motor -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, maximum output voltage can be set in motor controller, diodes and fuses avoid overvoltage, mitigation is possible	1	The supplier developed its motor controller according to applicable standards	*a*
	1.10.1	Electric motor becomes too hot	Motor controller reduces maximum engine torque or shuts electric motor down -> demanded steering angle cannot be provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only electric motor fails limited control over steering is given, emergency braking possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, prototype electric motor (and temperature sensor) that is also used in light aircrafts, motor controller monitors temperatures	*a*
	1.10.2		Overheating of electric motor -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, prototype electric motor (and temperature sensor) that is also used in light aircrafts, motor controller monitors temperatures	*a*
	1.11.1	Motor controller becomes too hot	Motor controller goes into safety shutdown -> demanded steering angle cannot be provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only electric motor fails limited control over steering is given, emergency braking possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its motor controller according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Steering unit	1.11.2	Motor controller becomes too hot	Motor controller fails to go into safety shut-down -> overheating of motor controller -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its motor controller according to applicable standards	*a*
	1.12.1	Water ingress at electric motor	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	1.12.2			Maintenance	1	Service engineer or mechanic may receive only minor injuries	1	Rare use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	1.12.3		Electric motor is unable to operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	1.13.1	Water ingress at motor controller	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	1.13.2			Maintenance	1	Service engineer or mechanic may receive only minor injuries	1	Rare use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Steering unit	1.13.3	Water ingress at motor controller	Motor controller is unable to operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	1.14	Motor controller provides no/incorrect/too late information to IPG Roadbox	IPG Roadbox is unable to calculate correct WMDS state -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no direct control over motor controller, no mitigation possible	1	The supplier developed its motor controller according to applicable standards	*a*
Drive unit	2.1	No or insufficient HV energy supply	Safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, HV energy cut is sudden and can hardly be detected prior to hazardous event, steering is possible, mitigation is possible	1	HV accumulator and safety-oriented battery management system with high availability	*a*
	2.2	No or insufficient LV energy supply	Safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, HV energy cut is sudden and can hardly be detected prior to hazardous event, steering is possible, mitigation is possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*
	2.3.1	HV input voltage too high	Motor controller goes into safety shutdown -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, diodes and fuses avoid overvoltage, mitigation is possible	2	HV accumulator cannot provide more than its maximum voltage, except when recuperation is in process.	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Drive unit	2.3.2	HV input voltage too high	Motor controller fails to go into safety shutdown -> overvoltage in power electronics -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, diodes and fuses avoid overvoltage, mitigation is possible	1	The supplier developed its motor controller according to applicable standards and equipped the controller with overvoltage protection	*a*
	2.3.3			Maintenance	1	Service engineer or mechanic may receive only minor injuries	1	Rare use case	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, diodes and fuses avoid overvoltage, mitigation is possible	1	The supplier developed its motor controller according to applicable standards and equipped the controller with overvoltage protection	*a*
	2.4.1	LV input voltage too high	Motor controller goes into safety shutdown -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by system operator (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*
	2.4.2		Motor controller fails to go into safety shutdown -> overvoltage in power electronics -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by system operator (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*
	2.5.1	Electric motor provides no/less/more torque than demanded	Incorrect torque leads to no/decreased/increased wheel hub torque and therefore incorrect acceleration/deceleration -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	Electric motor that is also used in light aircrafts, output voltage of motor controller translates directly to motor torque	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Drive unit	2.5.2	Electric motor provides no/less/more torque than demanded	Incorrect torque leads to no/decreased/increased wheel hub torque and therefore incorrect acceleration/deceleration -> safety logic detects failure -> emergency braking	Maintenance, service engineer(s) standing close by electric motor	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled service engineer, control inputs to the DS can be checked before executing them, mitigation is possible	1	Electric motor that is also used in light aircrafts, output voltage of motor controller translates directly to motor torque	*a*
	2.6	Resolver delivers no electric motor speed signal	Motor controller is unable to control motor torque -> demanded acceleration/deceleration cannot be provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	The supplier developed its resolver according to applicable standards	*a*
	2.7	Resolver delivers too low/high electric motor speed signal	Motor controller demand too high/low torque from electric motor -> too high/low motor torque -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	The supplier developed its resolver according to applicable standards	*a*
	2.8.1	Temperature sensor delivers no/too low/high electric motor temperature signals	Motor controller reduces maximum electric motor torque or shuts electric motor down -> demanded motor torque cannot be provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, can hardly be detected prior to hazardous event, if only one electric motor fails, limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	Electric motor (and temperature sensor) that is also used in light aircrafts	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Drive unit	2.8.2	Temperature sensor delivers no/too low/high electric motor temperature signals	Motor controller fails to reduce electric motor torque or to shut electric motor down -> overheating of electric motor -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Electric motor (and temperature sensor) that is also used in light aircrafts, motor controller developed according to applicable standards	*a*
	2.9.1	Motor controller provides no/too low/too high voltage to electric motor	No/too low/too high torque from electric motor -> demanded motor torque cannot be provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, detection possible by comparing the signals of all three steering motors, if only one electric motor fails, limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	The supplier developed its motor controller according to applicable standards	*a*
	2.9.2		Overvoltage in electric motor -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, maximum output voltage can be set in motor controller, diodes and fuses avoid overvoltage, mitigation is possible	1	The supplier developed its motor controller according to applicable standards	*a*
	2.10.1	Electric motor becomes too hot	Motor controller reduces maximum engine torque or shuts electric motor down -> demanded motor torque cannot be provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only one electric motor fails, limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, prototype electric motor (and temperature sensor) that is also used in light aircrafts, motor controller monitors temperatures	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Drive unit	2.10.2	Electric motor becomes too hot	Overheating of electric motor -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, prototype electric motor (and temperature sensor) that is also used in light aircrafts, motor controller monitors temperatures	*a*
	2.11.1	Motor controller becomes too hot	Motor controller goes into safety shutdown -> demanded motor torque cannot be provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, if only one electric motor fails, limited control over acceleration/deceleration is given, steering is possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its motor controller according to applicable standards	*a*
	2.11.2		Motor controller fails to go into safety shutdown -> overheating of motor controller -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its motor controller according to applicable standards	*a*
	2.12.1	Water ingress at electric motor	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	2.12.2			Maintenance	1	Service engineer or mechanic may receive only minor injuries	1	Rare use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Drive unit	2.12.3	Water ingress at electric motor	Electric motor is unable to operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	2.13.1	Water ingress at motor controller	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	2.13.2			Maintenance	1	Service engineer or mechanic may receive only minor injuries	1	Rare use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	2.13.3		Motor controller is unable to operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	2.14	Motor controller provides no/incorrect/too late information to IPG Roadbox	IPG Roadbox is unable to calculate correct WMDS state -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no direct control over motor controller, no mitigation possible	1	The supplier developed its motor controller according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Hexapod	3.1	No or insufficient HV power supply	Power electronics shut down -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, emergency shutdown and HV energy cut are sudden and can hardly be detected prior to hazardous event, rescue enabled by provided ladder, mitigation is possible	1	HV accumulator and safety-oriented battery management system with high availability	*a*
	3.2.1	HV input power too high	Power electronics goes into safety shutdown -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, mitigation is possible	1	HV accumulator cannot provide more than its maximum voltage, overvoltage by recuperation is avoided in motor controller and by a diode	*a*
	3.2.2		Power electronics fail to go into safety shutdown -> overvoltage at power electronics -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, HV overvoltage is sudden and can hardly be detected prior to hazardous event, recuperation can be avoided, mitigation is possible	1	The supplier developed its power electronics according to applicable standards	*a*
	3.3.1	Linear actuator provides no/less/more force than demanded	Motion of the linear actuators does not match the inverse kinematics model -> tension within hexapod may lead to fracture of actuator -> other actuators cannot support static and dynamic dome load -> restraining straps prevent dome from falling off the self-driving platform	Driving simulation with test person	1	Test person may be injured	2	Regular application	2	Skilled system operator, no direct control over inverse kinematics model or voltage provided to actuators, no mitigation possible	1	The suppliers developed their actuators according to applicable standards	*a*
	3.3.2			Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled service engineer/mechanic, no direct control over inverse kinematics model or voltage provided to actuators, service engineers and mechanics are instructed to stand back of WMDS when HV is switched on, mitigation is possible	1	The suppliers developed their actuators according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Hexapod	3.4	Linear actuator's position sensor delivers no signal	Power electronics cannot control the linear actuator's position -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, safe hexapod position can be reached with open-loop control, rescue enabled by provided ladder, mitigation is possible	1	The supplier developed its actuators and sensors according to applicable standards	*a*
	3.5	Linear actuator's position sensor delivers too low/high signal	Power electronics demands too high/low actuator force -> motion of the linear actuators does not match the inverse kinematics model -> tension within hexapod may lead to fracture of actuator -> other actuators cannot support static and dynamic dome load -> restraining straps prevent dome from falling off the self-driving platform	Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled service engineer/mechanic, no direct control over inverse kinematics model or voltage provided to actuators, service engineers and mechanics are instructed to stand back of WMDS when HV is switched on, mitigation is possible	1	The supplier developed its actuators and sensors according to applicable standards	*a*
	3.6.1	Linear actuator's temperature sensor delivers no/too low/high signal	Power electronics reduce maximum actuator force or shuts actuator down -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, temperatures can be monitored and compared, rescue enabled by provided ladder, mitigation is possible	1	The supplier developed its actuators and sensors according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Hexapod	3.6.2	Linear actuator's temperature sensor delivers no/too low/high signal	Power electronics fails to reduce maximum actuator force or to shut actuator down -> overheating of actuator -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored and compared, mitigation possible	1	The supplier developed its actuators and sensors according to applicable standards	*a*
	3.7.1	Power electronics provide no/too low/too high power to linear actuator	No/too low/too high force from one linear actuator -> motion of the linear actuators does not match the inverse kinematics model -> tension within hexapod may lead to fracture of actuator -> other actuators cannot support static and dynamic dome load -> restraining straps prevent dome from falling off the self-driving platform	Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled service engineer/mechanic, no direct control over inverse kinematics model or voltage provided to actuators, service engineers and mechanics are instructed to stand back of WMDS when HV is switched on, mitigation is possible	1	The supplier developed its power electronics according to applicable standards	*a*
	3.7.2		Too high force from all linear actuators -> acceleration of the hexapod above demanded acceleration	Driving simulation with test person	1	Test person may be injured	2	Regular application	2	Skilled system operator, no direct control over actuators, no mitigation possible	1	The supplier developed its power electronics according to applicable standards	*a*
	3.7.3		Overvoltage at linear actuator -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	2	Skilled system operator, no direct control over actuators, no mitigation possible	1	The supplier developed its power electronics according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Hexapod	3.8.1	Linear actuator becomes too hot	Power electronics reduces maximum actuator force or shuts actuator down -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, temperatures can be monitored, rescue enabled by provided ladder, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its actuators and sensors according to applicable standards	*a*
	3.8.2		Power electronics fails to reduce maximum actuator force or to shut actuator down -> overheating of actuator -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its actuators and sensors according to applicable standards	*a*
	3.9.1	Power electronics become too hot	Power electronics goes into safety shutdown -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, temperatures can be monitored, rescue enabled by provided ladder, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its power electronics according to applicable standards	*a*
	3.9.2		Power electronics fails to go into safety shutdown -> overheating of power electronics -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its power electronics according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Hexapod	3.10	The motion of one or more linear actuators, demanded by the power electronics, does not match the inverse kinematics model	Tension within hexapod may lead to fracture of actuator -> other actuators cannot support static and dynamic dome load -> restraining straps prevent dome from falling off the self-driving platform	Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled service engineer/mechanic, no direct control over actuators, service engineers and mechanics are instructed to stand back of WMDS when HV is switched on, mitigation is possible	1	The supplier developed its power electronics according to applicable standards	*a*
	3.11.1	Water ingress at linear actuator	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	3.11.2			Maintenance at hexapod	1	Service engineer or mechanic may receive only minor injuries	1	Maintenance at hexapod	1	Skilled service engineer and mechanic, water ingress can be observed, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	3.11.3			Emergency rescue	2	Test person might be seriously injured or even killed	1	Rare emergency use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Hexapod	3.11.4	Water ingress at linear actuator	Linear actuator is unable to operate -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, rescue enabled by provided ladder, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	3.12.1	Water ingress at power electronics	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	3.12.2		Power electronics is unable to operate -> demanded hexapod motion cannot be provided	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, rescue enabled by provided ladder, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	3.13	Power electronics provide no/incorrect/too late information to IPG Roadbox	IPG Roadbox is unable to calculate correct WMDS state -> hexapod motion is uncontrollable	Emergency rescue, dome fully tilted and poorly accessible	2	Test person's condition might worsen because rescue is impeded	1	Rare emergency use case	1	Skilled system operator, no direct control over power electronics, rescue enabled by provided ladder, mitigation is possible	1	The supplier developed its power electronics according to applicable standards	*a*
Mock-up	4.1.1	No or insufficient power supply	Test person is unable to give control inputs	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	2	Skilled system operator, energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.1.2	No or insufficient power supply	Test person is unable to communicate with system operator and vice versa	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	2	Skilled system operator, energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*
	4.1.3		Test person cannot receive system feedback through visual, auditory, and tactile channels	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	2	Skilled system operator, energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*
	4.1.4		Test person cannot receive system feedback through visual, auditory, and tactile channels -> test person gets motion sick and throws up onto E/E/PE element -> short circuit -> IMD cuts power supply -> test person must be rescued	Driving simulation with test person, dynamic driving situation	3	Test person and/or emergency personnel may be seriously injured or even killed	1	Regular use case, rare event	1	Skilled system operator, test person can be monitored and driving simulation can be aborted prior to critical event, mitigation is possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.1.5	No or insufficient power supply	System operator is unable to monitor test person	Driving simulation or emergency rescue with unclear situation for test person, test person might unbuckle and/or move within move	2	Test person may be seriously injured or even killed	1	Regular use case, rare event	1	Skilled system operator, energy cut is sudden and can hardly be detected prior to hazardous event, test person is instructed not to unbuckle unless he is told to do so, mitigation is possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*
	4.1.6			Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	2	Skilled system operator, energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*
	4.1.7		Air conditioning is unable to operate	Driving simulation with test person, extremely cold/hot environmental conditions	2	Frostbite/Heat stroke	1	Regular use case, rare event	1	Unskilled test person, when dome gets too cold/hot test person can leave DS, mitigation is possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut, extreme temperatures excluded from environmental conditions	*a*
	4.2.1	Input power too high	Control elements go into safety shutdown -> test person cannot give control inputs	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.2.2	Input power too high	Representation elements go into safety shutdown -> test person cannot receive system feedback through visual, auditory, and tactile channels	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*
	4.2.3		Communication system goes into safety shutdown -> test person is unable to communicate with system operator and vice versa	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	1	Regular use case, rare event	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*
	4.2.4		Surveillance system goes into safety shutdown -> system operator is unable to monitor test person	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	1	Regular use case, rare event	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.2.5	Input power too high	Air conditioning goes into safety shutdown -> air conditioning is unable to operate	Driving simulation with test person, extremely cold/hot environmental conditions	2	Frost-bite/Heat stroke	1	Regular use case, rare event	1	Unskilled test person, when dome gets too cold/hot test person can leave DS, mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage, extreme temperatures excluded from environmental conditions	*a*
	4.2.6		Any of the subsystem's elements fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular applications	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage, suppliers of subsystem's elements developed their components according to applicable standards	*a*
	4.3	Gear selection is not/not properly sensed	No/wrong gear selection is forwarded to WMDS dynamics control subsystem -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its gear selection system according to applicable standards	*a*
	4.4	Steering wheel angle is not/not properly sensed	No/wrong steering wheel angle is forwarded to WMDS dynamics control subsystem -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its steering wheel according to applicable standards	*a*
	4.5	Clutch pedal position is not/not properly sensed	No/wrong clutch pedal position is forwarded to WMDS dynamics control subsystem -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its pedal assembly according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.6	Brake pedal position is not/not properly sensed	No/wrong brake pedal position is forwarded to WMDS dynamics control subsystem -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its pedal assembly according to applicable standards	*a*
	4.7	Accelerator pedal position is not/not properly sensed	No/wrong accelerator pedal position is forwarded to WMDS dynamics control subsystem -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its pedal assembly according to applicable standards	*a*
	4.8	Steering wheel force feedback actuator gives no/too low/too high feedback force	False cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Unskilled test person, when false cues are represented test person can communicate with system operator and abort driving simulation, mitigation is possible	1	Supplier developed its steering wheel according to applicable standards	*a*
	4.9	Brake pedal's ABS shaker gives no/too low/too high feedback force	False cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Unskilled test person, when false cues are represented test person can communicate with system operator and abort driving simulation, mitigation is possible	1	Supplier developed its pedal assembly according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.10	Sound system gives no/wrong/ too early/too late auditory feedback	False cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Unskilled test person, when false cues are represented test person can communicate with system operator and abort driving simulation, mitigation is possible	1	Supplier developed its sound system according to applicable standards	*a*
	4.11	Visual representation system gives no/wrong/ too early/too late visual feedback	False cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Unskilled test person, when false cues are represented test person can communicate with system operator and abort driving simulation, mitigation is possible	1	Supplier developed its visual representation system according to applicable standards	*a*
	4.12	Air conditioning is set at too high/low air temperature	Temperature within dome is too low/high -> health hazard to test person	Driving simulation with test person	2	Frost-bite/Heat stroke	2	Regular application	1	Unskilled test person, when dome gets too cold/hot test person can communicate with system operator and abort driving simulation and leave DS, mitigation is possible	1	Skilled system operator sets temperature, supplier developed its air conditioning according to applicable standards	*a*
	4.13.1	Any of the representation elements becomes too hot	Representation element goes into safety shutdown -> test person cannot receive system feedback through visual, auditory, or tactile channels	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the suppliers developed their representation elements according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.13.2	Any of the representation elements becomes too hot	Representation element fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its power electronics according to applicable standards	*a*
	4.14.1	Any of the control elements becomes too hot	Control element goes into safety shutdown -> test person cannot give control inputs	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, temperatures and test person's control input and behaviour can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the suppliers developed their control input elements according to applicable standards	*a*
	4.14.2		Control element fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the suppliers developed their control input elements according to applicable standards	*a*
	4.15.1	Communication system becomes too hot	Communication system goes into safety shutdown -> test person is unable to communicate with system operator and vice versa	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its communication system according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.15.2	Communication system becomes too hot	Communication system fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its communication system according to applicable standards	*a*
	4.16.1	Surveillance system becomes too hot	Surveillance system goes into safety shutdown -> system operator is unable to monitor test person	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	1	Skilled system operator, test person can communicate with system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its surveillance system according to applicable standards	*a*
	4.16.2		Surveillance system fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its surveillance system according to applicable standards	*a*
	4.17.1	Air conditioning system becomes too hot	Air conditioning goes into safety shutdown -> air conditioning is unable to operate	Driving simulation with test person, extremely cold/hot environmental conditions	2	Frostbite/Heat stroke	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its air conditioning according to applicable standards	*a*
	4.17.2		Air conditioning fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular applications	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its air conditioning according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.18.1	Water ingress at visual representation system	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular applications	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.18.2		Visual representation system is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.19.1	Water ingress at sound system	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular applications	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.19.2		Sound system is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.20.1	Water ingress at steering wheel	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular applications	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.20.2		Steering wheel force feedback actuator is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.20.3	Water ingress at steering wheel	Steering wheel angle sensor is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.21.1	Water ingress at pedals	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular applications	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.21.2		Brake pedal ABS shaker is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.21.3		Brake and/or clutch and/or accelerator pedal sensor is unable to operate -> false cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person's control input and behaviour can be monitored, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.22.1	Water ingress at communication system	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.22.2	Water ingress at communication system	Communication system is unable to operate -> test person cannot communicate with system operator and vice versa	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	2	Regular applications	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.23.1	Water ingress at surveillance system	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.23.2		Surveillance system is unable to operate -> system operator cannot monitor test person	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.24.1	Water ingress at air conditioning	Short circuit -> IMD cuts power supply	Driving simulation with test person	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.24.2	Water ingress at air conditioning	Air conditioning is unable to operate -> health hazard to test person	Driving simulation with test person, extremely cold/hot environmental conditions	2	Frost-bite/Heat stroke	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, temperatures can be monitored, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	4.25	Communication system does not/other than/too late forward the test person's input to external command device's communication system	System operator cannot/too late react to the test person's input	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	1	Skilled system operator, test person can be monitored, mitigation is possible	2	Wireless data transmission, supplier developed its communication system according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Mock-up	4.26	Surveillance system does not/other than/too late forward its information to the external command device's communication system	System operator cannot/too late react to the test person's behaviour/condition	Driving simulation with test person, test person has a health issue	2	Test person's condition might worsen because rescue is impeded	1	Regular use case, rare event	1	Skilled system operator, test person can communicate with system operator, mitigation is possible	2	Wireless data transmission, supplier developed its surveillance system according to applicable standards	*a*
	4.27	Driver input not/incorrectly/too late forwarded to IPG Roadbox	False cues are generated	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	1	Skilled system operator, test person and signals can be monitored, mitigation is possible	1	Supplier developed its components according to applicable standards	*a*
Ext. com. Dev.	5.1.1	No or insufficient power supply	Safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Power cut from stationary power socket very unlikely	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
External command device	5.1.2	No or insufficient power supply	Safety logic detects failure -> emergency braking	Manual drive, maximum manually adjustable driving velocity	3	Test person and/or bystanders and/or system operator may be injured and/or killed	1	Rare use case	1	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, system operator is instructed to reduce the driving velocity when driving close to the workspace boundaries	1	Power cut from stationary power socket very unlikely	*a*
	5.1.3		External command device is unable to operate -> communication with and surveillance of test person impossible	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	1	Regular application, rare event	1	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, test person is instructed not to unbuckle unless he is told to do so, mitigation is possible	1	Power cut from stationary power socket very unlikely	*a*
	5.2.1	Input power too high	External command device goes into safety shutdown -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, overvoltage in stationary power supply only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	Overvoltage stationary power socket very unlikely	*a*
	5.2.2		External command device fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation with test person	1	System operator may receive only minor injuries	2	Regular application	1	Skilled system operator, overvoltage in stationary power supply only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	Overvoltage stationary power socket very unlikely	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
External command device	5.2.3	Input power too high	External command device fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Maintenance	1	Service engineer or mechanic may receive only minor injuries	1	Rare use case	1	Skilled system operator, overvoltage in stationary power supply only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	Overvoltage stationary power socket very unlikely	*a*
	5.3.1	Water ingress at external command device	Short circuit -> IMD cuts power supply	Driving simulation	1	System operator may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	5.3.2		External command device is unable to operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	5.3.3		External command device is unable to operate -> communication with and surveillance of test person impossible	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	1	Regular application, rare event	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, test person is instructed not to unbuckle unless he is told to do so, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
External command device	5.4.1	External command device becomes too hot	External command device goes into safety shutdown -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its external command device according to applicable standards	*a*
	5.4.2		External command device fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation	1	System operator may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its external command device according to applicable standards	*a*
	5.5	Command inputs are not/incorrectly/too late forwarded to the WMDS dynamics control subsystem	System operator has no/wrong/delayed influence on DS trajectory -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no mitigation possible	1	Secured wireless data transmission, supplier developed its external command device according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
External command device	5.6	Communication system does not/other than/too late forward the system operator's input to the mock-up E/E/PE subsystem's communication system	Test person cannot/too late react to the system operator's input	Driving simulation or emergency rescue with unclear situation for test person, test person must not unbuckle and/or move within dome	2	Test person may be seriously injured or even killed	2	Regular applications	1	Unskilled test person, no communication possible, test person is instructed not to unbuckle unless he is told to do so, mitigation is possible	1	Secured wireless data transmission, supplier developed its external command device according to applicable standards	*a*
WMDS dynamics control	6.1	No or insufficient LV power supply	Safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*
	6.2.1	LV input power too high	IPG Roadbox goes into safety shutdown -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*
	6.2.2		ADMA G-3 goes into safety shutdown -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), emergency braking is possible, mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
WMDS dynamics control	6.2.3	LV input power too high	IPG Roadbox and/or ADMA G-3 fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*
	6.3.1	Water ingress at IPG Roadbox	Short circuit -> IMD cuts power supply	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	6.3.2		IPG Roadbox is unable to operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	6.4.1	Water ingress at ADMA G-3	Short circuit -> IMD cuts power supply	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	6.4.2		ADMA-G3 is unable to operate -> position/motion of DS unclear -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	6.5.1	IPG Roadbox becomes too hot	IPG Roadbox goes into safety shutdown -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its Roadbox according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
WMDS dynamics control	6.5.2	IPG Roadbox becomes too hot	IPG Roadbox fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its Roadbox according to applicable standards	*a*
	6.6.1	ADMA G-3 becomes too hot	ADMA G-3 goes into safety shutdown -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, open-loop control still possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its ADMA G-3 according to applicable standards	*a*
	6.6.2		ADMA G-3 fails to go into safety shutdown -> short circuit -> IMD cuts power supply	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, open-loop control still possible, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its ADMA G-3 according to applicable standards	*a*
	6.7	ADMA G-3 signals are not/incorrectly/too late forwarded to IPG Roadbox	Position/motion of DS unclear -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, open-loop control still possible, emergency braking possible, mitigation is possible	1	Supplier developed its ADMA G-3 according to applicable standards	*a*
	6.8	IPG Roadbox signals are not/incorrectly/too late forwarded to steering unit subsystem	Incorrect steering angle is provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, emergency braking possible, mitigation is possible	1	Supplier developed its IPG Roadbox according to applicable standards, self-programmed dynamics control externally reviewed and thoroughly tested	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
WMDS dynamics control	6.9	IPG Roadbox signals are not/incorrectly/too late forwarded to drive unit subsystem	Maximum wheel hub torque is provided -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no mitigation possible	1	Supplier developed its IPG Roadbox according to applicable standards, self-programmed dynamics control externally reviewed and thoroughly tested	*a*
	6.10	IPG Roadbox signals are not/incorrectly/too late forwarded to hexapod subsystem	Incorrect linear actuator force is provided -> false cues are generated and/or motion of the linear actuators does not match the inverse kinematics model -> tension within hexapod may lead to fracture of actuator -> other actuators cannot support static and dynamic dome load -> restraining straps prevent dome from falling off the self-driving platform	Maintenance at hexapod	3	Service engineer(s) and/or mechanic(s) may be seriously injured or even killed	1	Rare use case	1	Skilled service engineers and mechanics, service engineers and mechanics are instructed to stand back of WMDS when HV is switched on, mitigation is possible	1	Supplier developed its IPG Roadbox according to applicable standards, self-programmed dynamics control externally reviewed and thoroughly tested	*a*
	6.11	IPG Roadbox signals are not/incorrectly/too late forwarded to mock-up subsystem	Test person cannot receive system feedback through visual, auditory, and tactile channels	Driving simulation with test person, dynamic driving situation	1	Motion sickness	2	Regular application	2	Skilled system operator, no mitigation possible	1	Supplier developed its IPG Roadbox according to applicable standards, self-programmed dynamics control externally reviewed and thoroughly tested	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
WMDS dynamics control	6.12	IPG Roadbox signals are not/incorrectly/too late forwarded to external command device subsystem	Safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no mitigation possible	1	Secured wireless data transmission, supplier developed its IPG Roadbox according to applicable standards, self-programmed dynamics control externally reviewed and thoroughly tested	*a*
	6.13	ADMA G-3 position and/or motion are not/incorrectly measured	Position/motion of DS unclear -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, emergency braking possible, mitigation is possible	2	sensor noise, sensor drift, GPS is blind	*a*
Power supply	7.1	Traction battery's management system cuts power supply	Safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no direct control over battery management system, no mitigation possible	1	HV accumulator and safety-oriented battery management system with high availability	*a*
	7.2	Auxiliary battery's management system cuts power supply	Safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no direct control over battery management system, no mitigation possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Power supply	7.3.1	Overvoltage from traction battery	Steering unit, drive unit, and hexapod E/E/PE subsystems cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no direct control over battery management system, no mitigation possible	1	HV accumulator cannot provide more than its maximum voltage	*a*
	7.3.2		Possibly short circuit at steering unit, drive unit, and hexapod E/E/PE subsystems -> fuse blows	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, no direct control over battery management system, diodes and fuses avoid overvoltage, mitigation is possible	1	HV accumulator cannot provide more than its maximum voltage	*a*
	7.4.1	Overvoltage from auxiliary battery	Steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its maximum voltage	*a*
	7.4.2		Possibly short circuit at steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems -> fuse blows	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by test person (when a thunderstorm rises), diodes and fuses avoid overvoltage, mitigation is possible	1	LV accumulator cannot provide more than its maximum voltage	*a*
	7.5.1	Overvoltage from AC/DC converter	Mock-up E/E/PE subsystem cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no direct control over AC/DC converter, no mitigation possible	1	LV accumulator cannot provide more than its maximum voltage, supplier developed its AC/DC converter according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Power supply	7.5.2	Overvoltage from AC/DC converter	Possibly short circuit at mock-up E/E/PE subsystem -> fuse blows	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, no direct control over AC/DC converter, diodes and fuses avoid overvoltage, mitigation is possible	1	LV accumulator cannot provide more than its maximum voltage, supplier developed its AC/DC converter according to applicable standards	*a*
	7.6.1	Overvoltage from stationary power connection	External command device E/E/PE subsystem cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, overvoltage in stationary power supply only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	Overvoltage from power socket very unlikely, diodes and fuses avoid overvoltage	*a*
	7.6.2		Possibly short circuit at external command device E/E/PE subsystem -> fuse blows	Driving simulation	1	System operator may receive only minor injuries	2	Regular application	1	Skilled system operator, overvoltage in stationary power supply only possible with lightning which can be avoided by test person (when a thunderstorm rises), mitigation is possible	1	Overvoltage from power socket very unlikely, diodes and fuses avoid overvoltage	*a*
	7.7.1	Overvoltage from steering unit/drive unit E/E/PE subsystem when recuperating	Traction battery goes into safety shutdown -> steering unit, drive unit, and hexapod E/E/PE subsystems cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, recuperation can be avoided, mitigation is possible	1	Recuperation current is limited in motor controller, diodes and fuses avoid overvoltage, motor controller is developed by its supplier according to applicable standards	*a*
	7.7.2		Traction battery fails to go into safety shutdown -> short circuit -> fuse blows	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, recuperation can be avoided, mitigation is possible	1	Recuperation current is limited in motor controller, diodes and fuses avoid overvoltage, motor controller is developed by its supplier according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Power supply	7.8.1	Water ingress at traction battery	Steering unit, drive unit, and hexapod E/E/PE subsystems cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	7.8.2		Possibly short circuit at steering unit, drive unit, and hexapod E/E/PE subsystems -> fuse blows	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	7.9.1	Water ingress at auxiliary battery	Steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	7.9.2		Possibly short circuit at steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems -> fuse blows	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	7.10.1	Water ingress at AC/DC converter	Mock-up E/E/PE subsystem cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	7.10.2		Possibly short circuit at mock-up E/E/PE subsystem -> fuse blows	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Power supply	7.11.1	Water ingress at stationary power connection	WMDS dynamics control E/E/PE subsystem cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	7.11.2		Possibly short circuit at external command device E/E/PE subsystem -> Fuse blows	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*
	7.12.1	Traction battery becomes too hot	Traction battery goes into safety shutdown -> steering unit, drive unit, and hexapod E/E/PE subsystems cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its Roadbox according to applicable standards	*a*
	7.12.2		Traction battery fails to go into safety shutdown -> Short circuit at steering unit, drive unit, and hexapod E/E/PE subsystems -> IMD cuts power supply	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its Roadbox according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Power supply	7.13.1	Auxiliary battery becomes too hot	Auxiliary battery goes into safety shutdown -> steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its Roadbox according to applicable standards	*a*
	7.13.2		Auxiliary battery fails to go into safety shutdown -> possibly short circuit at steering unit, drive unit, mock-up, and WMDS dynamics control E/E/PE subsystems -> IMD cuts power supply	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its Roadbox according to applicable standards	*a*
	7.14.1	AC/DC converter becomes too hot	AC/DC converter goes into safety shutdown -> mock-up E/E/PE subsystem cannot operate -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its Roadbox according to applicable standards	*a*
	7.14.2		AC/DC converter fails to go into safety shutdown -> possibly short circuit at mock-up E/E/PE subsystem -> IMD cuts power supply	Driving simulation	1	Test person may receive only minor injuries	2	Regular application	1	Skilled system operator, temperatures can be monitored, mitigation is possible	1	Extreme heat excluded from environmental conditions, the supplier developed its Roadbox according to applicable standards	*a*

Subsys.	No.	HAZARDOUS EVENTS			CLASSIFICATION OF HAZARDOUS EVENTS								SIL
		Hazard		Situation	C	Justif.	F	Justif.	P	Justification	W	Justification	
		Failure	Consequence										
Power supply	7.15	Traction battery's SOC is not/incorrectly/too late transmitted to WMDS dynamics control system	System operator is unaware of traction battery's SOC -> WMDS may run out of HV power -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no mitigation is possible	1	Supplier developed its battery management system according to applicable standards	*a*
	7.16	Auxiliary battery's SOC is not/incorrectly/too late transmitted to WMDS dynamics control system	System operator is unaware of auxiliary battery's SOC -> WMDS may run out of LV power -> safety logic detects failure -> emergency braking	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no mitigation is possible	1	Supplier developed its battery management system according to applicable standards	*a*

C.4 Preliminary Hazard List for an Exemplary Application of the Safety Architecture

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
Power supply	7.17	Incorrect measurement of any IMD	Short circuit is not detected -> Possibly fire hazard	Driving simulation with test person, test person must be rescued from dome	3	Test person and/or emergency personnel may be seriously injured or even killed	1	Regular application, rare event	1	Skilled system operator, no control over IMD, diodes and fuses avoid overvoltage, mitigation is possible	1	Supplier developed its IMD according to applicable standards, self-diagnosis integrated	*a*	Short circuit must be reliably detected by IMDs
	7.18	No or insufficient LV power supply at any IMD	IMD inoperable -> no "OK"-signal to external emergency braking E/E/PE subsystem -> emergency braking activated	Maintenance, system engineer(s) and/or mechanic(s) working at power supply subsystem	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	1	Skilled system engineers and mechanics, system engineers and mechanics are instructed to stand back from operational emergency braking system, V energy cut is sudden and can hardly be detected prior to hazardous event, mitigation is possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*	LV power supply must not be cut
	7.19	LV input power too high at any IMD	IMD inoperable -> no "OK"-signal to external emergency braking E/E/PE subsystem -> emergency braking activated	Maintenance, system engineer(s) and/or mechanic(s) working at power supply subsystem	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by system operator (when a thunderstorm rises), emergency braking is possible, mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*	LV power supply must not exceed nominal voltage
	7.20	Any fuse does not blow although it should	Continuous short circuit -> possibly fire hazard	Maintenance, system engineer(s) and/or mechanic(s) working at power supply subsystem, Overvoltage	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by system operator (when a thunderstorm rises), mitigation is possible	1	Supplier developed its fuses according to applicable standards, overvoltage in general unlikely	*a*	Fuses must reliably blow at threshold current

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
External emergency braking system	8.1.1	No or insufficient LV power supply	Programmable Logic Controller (PLC) cannot provide LV power to electric holding magnet -> emergency braking activated	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, LV energy cut is sudden and can hardly be detected prior to hazardous event, no mitigation possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*a*	LV power supply must not be cut
	8.1.2			Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	2	Skilled system engineers and mechanics, energy cut is sudden and can hardly be detected prior to hazardous event, mitigation is possible	1	Standard LV accumulator and standard battery management system make LV power cut more unlikely than HV power cut	*1*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated
	8.2.1	LV input power too high	PLC goes into safety shutdown -> no power provided to electric holding magnet -> emergency braking activated	Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by system operator (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated
	8.2.2		PLC fails to go into safety shutdown -> short circuit -> IMD cuts power supply -> no power provided to electric holding magnet -> emergency braking activated	Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	1	Skilled system operator, overvoltage only possible with lightning which can be avoided by system operator (when a thunderstorm rises), mitigation is possible	1	LV accumulator cannot provide more than its nominal voltage	*a*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
External emergency braking system	8.3.1	Water ingress at PLC	PLC cannot operate -> no power provided to electric holding magnet -> emergency braking activated	Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated
	8.3.2		Possibly short circuit at PLC -> IMD cuts power supply -> no power provided to electric holding magnet -> emergency braking activated	Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	1	Skilled system operator, if rain/snow etc. arises the system operator can take countermeasures, mitigation is possible	1	Environmental conditions exclude high humidity and water	*a*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated
	8.4.1	Electric holding magnet malfunctions/provides no or too low force	Emergency braking is activated	Driving simulation with test person, high velocity	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no influence on electric holding magnet, no mitigation possible	1	Supplier developed its magnet according to applicable standards, contact surface cleaned and smoothed during maintenance	*a*	Electric holding magnet must not provide no/too low force
	8.4.2			Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	2	Skilled system operator, no influence on electric holding magnet, no mitigation possible	1	Supplier developed its magnet according to applicable standards, contact surface cleaned and smoothed during maintenance	*1*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
External emergency braking system	8.5	Electric holding magnet provides too high force	Clamping force higher than needed, emergency braking activation may need longer (<< 1 s) than usual	Emergency situation, emergency braking is activated	1	Minor injuries because of unexpected deceleration	2	Regular application	2	Skilled system operator, no influence on electric holding magnet, no mitigation possible	1	Supplier developed its magnet according to applicable standards, contact surface cleaned and smoothed during maintenance	*a*	Electric holding magnet must not provide too high force
	8.6	Steel coil spring has not been preloaded	Brake pad has contact to underground -> undesired trajectory	Driving simulation initialisation with high dynamic motion at beginning	1	Minor injuries because of unexpected deceleration	1	Regular application, rare event	1	Skilled system operator, state of external emergency braking system can be checked visually beforehand, mitigation is possible	1	Human failure, conduct guidelines instruct system operator to check emergency braking system	*a*	Steel coil springs must always be preloaded prior to driving simulation initialisation
	8.7	No/too late signal from IMD	Sampling rate threshold is violated -> PLC activates emergency braking system	Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	2	Skilled system engineers and mechanics, no control over IMD, no mitigation possible	1	Supplier developed its IMD according to applicable standards	*1*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated
	8.8	No/too late signal from motor controller	Sampling rate threshold is violated -> PLC activates emergency braking system	Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	2	Skilled system engineers and mechanics, no direct control over motor controllers, no mitigation possible	1	Supplier developed its motor controller according to applicable standards	*1*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated

Subsys.	No.	HAZARDOUS EVENT			CLASSIFICATION OF HAZARD								SIL	Safety function
		Hazard		Situation	C	Justification	F	Justific.	P	Justification	W	Justification		
		Failure	Consequence											
External emergency braking system	8.9	No/too late signal from IPG Roadbox	Sampling rate threshold is violated -> PLC activates emergency braking system	Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	2	Skilled system engineers and mechanics, no direct control over IPG Roadbox, no mitigation possible	1	Supplier developed its IPG Roadbox according to applicable standards	*1*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated
	8.10	No/too late signal from external command device	Sampling rate threshold is violated -> PLC activates emergency braking system	Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	2	Skilled system engineers and mechanics, no direct control over external command device, no mitigation possible	1	Supplier developed its external command device according to applicable standards	*1*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated
	8.11	Unintended emergency signal by manual emergency stop	Emergency braking is activated	Maintenance, system engineer(s) and/or mechanic(s) standing close to emergency braking system	3	System engineer(s) and/or mechanic(s) might be seriously injured or even killed	1	Rare application	1	Skilled system engineers and mechanics, system engineers and mechanics are instructed to stand back from operational emergency braking system, mitigation is possible	1	Supplier developed its manual emergency stop according to applicable standards	*a*	System engineer(s) and/or mechanic(s) must not be injured or even killed when emergency braking is activated

Bibliography

Albrecht, T. et al.: Advanced Design Project, Fahrwiderstands- und Energiebedarfsbetrachtung des MORPHEUS (2016)
Albrecht, Torben; Davoodi, Aschkan; Wilczynski, David; Betancourt Bautista, Miguel A.; Huber, Katharina: Fahrwiderstands- und Energiebedarfsbetrachtung des MORPHEUS unter Berücksichtigung der speziellen Eigenschaften der Bandagenreifen, Advanced Design Project
Technische Universität Darmstadt, Darmstadt, Germany, 2016

Ammon, D.; Schiehlen, W.: Advanced Road Vehicles: Control Technologies (2009)
Ammon, Dieter; Schiehlen, Werner: Advanced Road Vehicles: Control Technologies, Driver Assistance, in: Schiehlen, Werner et al. (Eds.): Dynamical Analysis of Vehicle Systems, CISM International Centre for Mechanical Sciences Nr. 497, Springer, Vienna, Austria, 2009

Baumann, G. et al.: How to Build Europe's Largest Eight-Axes DS (2012)
Baumann, Gerd; Riemer, Thomas; Liedecke, Christoph; Rumbolz, Philip; Schmidt, Andreas: How to Build Europe's Largest Eight-Axes Motion Simulator, in: Espié, Stéphane; Kemeny, Andras; Mérienne, Frédéric (Eds.): Proceedings of the Driving Simulation Conference Europe 2012 (DSC), Actes INRETS A 134, INRETS, Bron, France, 2012

Baumann, G. et al.: The New DS of Stuttgart University (2012)
Baumann, Gerd; Riemer, Thomas; Liedecke, Christoph; Rumbolz, Philip; Schmidt, Andreas; Piegsa, Anne: The New Driving Simulator of Stuttgart University, in: ATZlive (Ed.): Proceedings of the 12th Stuttgart International Symposium Automotive and Engine Technology, Wiesbaden, Germany, 2012

Beidl, C.: Lecture Notes Combustion Engines II (2017)
Beidl, Christian: Lecture Notes Combustion Engines II, Darmstadt, Germany, 2017

Bel Power Solutions: 700DNC40-12-xG DC/DC Converter Data Sheet (2017)
Bel Power Solutions: 700DNC40-12-xG DC/DC Converter Data Sheet;
https://www.mouser.com/ds/2/643/bcd.00293_ae_700dnc40-12-xg-1116173.pdf, 2017, Access 07.03.2018

Berg, G.; Färber, B.: Vehicle in the Loop (2015)
Berg, Guy; Färber, Berthold: Vehicle in the Loop, in: Winner, Hermann (Ed.): Handbuch Fahrerassistenzsysteme, ATZ, Vieweg+Teubner, Wiesbaden, Germany, 2015

Betz, A. et al.: Concept Analysis of a WMDS (2012)
Betz, Alexander; Hämisch, Robert; Müller, Marius; Winner, Hermann: Concept Analysis of a Wheeled Mobile Driving Simulator Showing an Omnidirectional Motion Base for Urban Traffic Simulation, in: Proceedings of the 16th Berechnung, Simulation und Erprobung im Fahrzeugbau (SIMVEC), VDI-Berichte Nr. 2169, VDI, Düsseldorf, Germany, 2012

Betz, A. et al.: Motion Analysis of a WMDS (2012)
Betz, Alexander; Winner, Hermann; Ancochea, Marc; Graupner, Maren: Motion Analysis of a Wheeled Mobile Driving Simulator for Urban Traffic Situations, in: Espié, Stéphane; Kemeny, Andras; Mérienne, Frédéric (Eds.): Proceedings of the Driving Simulation Conference Europe 2012 (DSC), Actes INRETS A 134, INRETS, Bron, France, 2012

Betz, A. et al.: Driving Dynamics Control of a WMDS (2013)
Betz, Alexander; Butry, Andreas; Junietz, Philipp; Wagner, Paul; Winner, Hermann: Driving Dynamics Control of a Wheeled Mobile Driving Simulator Utilizing an Omnidirectional Motion Base for Urban Traffic Simulation, in: Proceedings of the Future Active Safety Technology Toward Zero-Traffic-Accident (fast-zero) 2013, 2013

Betz, A. et al.: Development and Validation of a Safety Architecture of a WMDS (2014)
Betz, Alexander; Wagner, Paul; Albrecht, Torben; Winner, Hermann: Development and Validation of a Safety Architecture of a Wheeled Mobile Driving Simulator, in: Kemeny, Andras; Espié, Stéphane; Mérienne, Frédéric (Eds.): Proceedings of the Driving Simulation Conference Europe 2014 (DSC), 2014

Betz, A. et al.: Konzeptanalyse und Erprobung eines WMDS (2014)
Betz, Alexander; Wagner, Paul; Scheibe, Thomas; Winner, Hermann: Konzeptanalyse und Erprobung eines selbstfahrenden Fahrsimulators für die Simulation von Stadtverkehr, in: Proceedings of the 17th Simulation und Erprobung in der Fahrzeugentwicklung (SIMVEC), VDI, Düsseldorf, Germany, 2014

Betz, A.: Diss., Feasibility Analysis and Design of WMDS (2015)
Betz, Alexander: Feasibility Analysis and Design of Wheeled Mobile Driving Simulators for Urban Traffic Simulation, Dissertation Technische Universität Darmstadt, Fortschrittberichte VDI: Reihe 12, Issues 786, VDI, Düsseldorf, Germany, 2015

Betz, A.; Winner, H.: Patent Knee Lever Safety System (2014)
Betz, Alexander; Winner, Hermann: Fahrzeug mit einer omnidirektionalen Antriebseinrichtung, Technische Universität Darmstadt, 64289, Darmstadt, DE, Patent DE102014108387A1, Patent application number: 102014108387, 2014

Blana, E.: A Survey of DS Around the World (1996)
Blana, Evi: A Survey of Driving Research Simulators Around the World, Leeds, UK, 1996

Boer, E. R. et al.: The Role of DS in Developing and Evaluating AD (2015)
Boer, Erwin R.; Penna, Mauro D.; Utz, Hans; Pedersen, Liam; Siehuis, Maarten: The Role of Driving Simulators in Developing and Evaluating Autonomous Vehicles, in: Bülthoff, Heinrich; Kemeny, Andras; Pretto, Paolo (Eds.): Proceedings of the Driving Simulation Conference & Exhibition Europe 2015 (DSC), Tübingen, Germany, 2015

Breuer, B.; Bill, K. H.: Bremsenhandbuch (2012)
Breuer, Bert; Bill, Karlheinz H.: Bremsenhandbuch, ATZ, Vieweg+Teubner, Wiesbaden, Germany, 2012

Bülthoff, H. et al.: DSC Europe 2015 (2015)
Bülthoff, Heinrich; Kemeny, Andras; Pretto, Paolo (Eds.) Proceedings of the Driving Simulation Conference & Exhibition Europe 2015 (DSC), Tübingen, Germany, 2015

Chapron, T.; Colinot, J.-P.: The New PSA Advanced DS (2007)
Chapron, Thomas; Colinot, Jean-Pierre: The New PSA Peugeot-Citroën Advanced Driving Simulator Overall Design and Motion Cue Algorithm, in: Proceedings of the Driving Simulator Conference North America 2007 (DSC), 2007

Clark et al.: NADS Motion System (2001)
Clark; Allen; Sparks; Hugh; Carmein; Judy: Unique Features and Capabilities of the NADS Motion System, in: Proceedings of the 17th International Technical Conference on the Enhanced Safety of Vehicles (ESV), 2001

Csillag, A.: Atlas of the Sensory Organs (2005)
Csillag, András: Atlas of the Sensory Organs, Humana Press, Totowa, NJ, USA, 2005

Dagdelen, M. et al.: MPC based MCA (2004)
Dagdelen, Mehmet; Reymond, Gilles; Kemeny, Andras; Bordier, Marc; Maizi, Nadia: MPC Based Motion Cueing Algorithm: Development and Application to the ULTIMATE Driving Simulator, in: Gauriat, Pierre; Kemeny, Andras (Eds.): Proceedings of the Driving Simulation Conference Europe 2004 (DSC), INRETS, Arcueil, France, 2004

Deutsches Institut für Normung e. V.: ISO 8855 (2013)
Deutsches Institut für Normung e. V.: Straßenfahrzeuge - Fahrzeugdynamik und Fahrverhalten - Begriffe, Beuth, Berlin, Germany, 2013

Donges, E.: Fahrsimulator (2001)
Donges, Edmund: Fahrsimulator, Bayrische Motoren Werke AG, Patent DE000010106150A1, Patent application number: 101 06 150.1, 2001

Ericson, C. A.: Hazard Analysis Techniques for System Safety (2005)
Ericson, Clifton A.: Hazard Analysis Techniques for System Safety, Wiley-Interscience, Hoboken, NJ, USA, 2005

Espié, S. et al.: DSC Europe 2012 (2012)
Espié, Stéphane; Kemeny, Andras; Mérienne, Frédéric (Eds.) Proceedings of the Driving Simulation Conference Europe 2012 (DSC), Actes INRETSA 134, INRETS, Bron, France, 2012

Fischer, M.: Diss., MCA für eine realitätsnahe Bewegungssimulation (2009)
Fischer, Martin: Motion-Cueing-Algorithmen für eine realitätsnahe Bewegungssimulation, Dissertation Technische Universität Carolo-Wilhelmina zu Braunschweig, Berichte aus dem DLR-Institut für Verkehrssystemtechnik, Issues 5, Deutsches Zentrum für Luft- und Raumfahrt e.V., Braunschweig, Germany, 2009

Fisher, D. L.: Handbook of DS (2011)
Fisher, Donald L.: Handbook of Driving Simulation for Engineering, Medicine, and Psychology, CRC Press, Boca Raton, 2011

Gietelink, O. et al.: VEHIL: A Test Facility for ADAS (2004)
Gietelink, Olaf; Ploeg, Jeroen; Schutter, Bart d.; Verhaegen, Michel: VEHIL: A Test Facility for Validation of Fault Management Systems for Advanced Driver Assistance Systems, in: Proceedings of the 1st IFAC Symposium on Advances in Automotive Control (AAC), 2004

Glatzki, F.: Bachelor's thesis, Trajektorienüberlagerung und Lenkleistungsbedarf eines WMDS (2016)
Glatzki, Felix: Untersuchung des Einflusses einer Trajektorienüberlagerung auf den Lenkleistungsbedarf eines selbstfahrenden Fahrsimulators, Bachelor's thesis
Technische Universität Darmstadt, Darmstadt, Germany, 2016

Gong, Z.; Konigorski, U.: Dynamic Modeling and Controller Design of WMDS (2016)
Gong, Zhongyi; Konigorski, Ulrich: Dynamic Modeling and Controller Design of an Omniwheel Mobile Platform by Differential Parameterization, in: Proceedings of the 15th European Control Conference (ECC), IEEE, Piscataway, NJ, USA, 2016

Gong, Z.; Konigorski, U.: Model-Based Control of a WMDS (2016)
Gong, Zhongyi; Konigorski, Ulrich: Model-Based Control of a Wheeled Mobile Driving Simulator, in: Kemeny, Andras et al. (Eds.): Proceedings of the Driving Simulation & Virtual Reality Conference & Exhibition Europe 2016 (DSC), 2016

Gong, Z.; Konigorski, U.: Comparison of Different MCA in a WMDS (2017)
Gong, Zhongyi; Konigorski, Ulrich: Comparison of Different Motion Cueing Algorithms in a Wheeled Mobile Driving Simulator, in: Kemeny, Andras et al. (Eds.): Proceedings of the Driving Simulation & Virtual Reality Conference & Exhibition Europe 2017 (DSC), 2017

Gong, Z.; Konigorski, U.: Modeling and Control of a WMDS (2017)
Gong, Zhongyi; Konigorski, Ulrich: Modeling and Control of a Wheeled Mobile Vehicle Driving Simulator by Differential Parameterization, in: Proceedings of the American Control Conference 2017 (ACC), IEEE, Piscataway, NJ, USA, 2017

Gough, V. E.; Whitehall, S. G.: Universal Tyre Test Machine (1962)
Gough, Vernon E.; Whitehall, S. G.: Universal Tyre Test Machine, in: Proceedings of 9th FISITA International Technical Congress, 1962

Graubohm, R. et al.: Systematic Design Considering Functional Safety Aspects (2017)
Graubohm, Robert; Stolte, Torben; Bagschik, Gerrit; Reschka, Andreas; Maurer, Markus: Systematic Design of Automated Driving Functions Considering Functional Safety Aspects, in: Proceedings of the 8th Tagung Fahrerassistenz, 2017

Graupner, M.: Bachelor's thesis, Entwicklung eines repräsentativen Stadtparcours (2011)
Graupner, Maren: Entwicklung eines repräsentativen Stadtparcours mittels makroskopischer Betrachtung lokaler Verkehrsbereiche, Bachelor's thesis
Technische Universität Darmstadt, Darmstadt, Germany, 2011

Greenberg, J. et al.: Lateral Motion Cues During Simulated Driving (2003)
Greenberg, Jeff; Artz, Bruce; Cathey, Larry: The Effect of Lateral Motion Cues During Simulated Driving, in: Proceedings of the Driving Simulator Conference North America 2003 (DSC), 2003

Groen, E. et al.: Psychophysical Thresholds of Linear Acceleration (2000)
Groen, Eric; Clari, Mario; Hosman, Ruud: Psychophysical Thresholds Associated with the Simulation of Linear Acceleration, in: Proceedings of the AIAA Modeling and Simulation Technologies Conference 2000, AIAA, Reston, VI, USA, 2000

Hajek, H.: Diss., Längsdynamik von elektrifizierten Straßenfahrzeugen (2017)
Hajek, Hermann: Längsdynamik und Antriebsakustik von elektrifizierten Straßenfahrzeugen – Beschreibung und Gestaltung des emotionalen Erlebens, Dissertation Technische Universität München, 2017

Hein, E. et al.: Advanced Design Project, Entwicklung des unskalierten WMDS (2017)
Hein, Eric; Lamrabet, Youssef; Niess, Sammy; Schmeiß, Mirco: Entwicklung des selbstfahrenden Fahrsimulators MORPHEUS 2.0, Advanced Design Project
Technische Universität Darmstadt, Darmstadt, Germany, 2017

Hettinger, L. J.; Riccio, G. E.: Visually Induced Motion Sickness (1992)
Hettinger, Lawrence J.; Riccio, Gary E.: Visually Induced Motion Sickness in Virtual Environments, in: Presence: Teleoperators and Virtual Environments (3), Issues1, pp. 306–310, 1992

Honda Deutschland: Honda R&D DS (2017)
Honda Deutschland: Honda R&D führt revolutionären Fahrsimulator ein, 2017

Hüsing, K.: Fahrsimulator (2001)
Hüsing, Kurt: Fahrsimulator, Bayerische Motoren Werke AG, Patent DE000010158101A1, Patent application number: 101 58 101.7, 2001

IEC TC 44 - Safety of machinery - electrotechnical aspects: IEC 62061 (2005)
IEC TC 44 - Safety of machinery - electrotechnical aspects: , IEC 1: Safety of Machinery - Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems, IEC, Geneva, Switzerland, 2005

IEC TC 56 - Dependability: IEC 60812 (2006)
IEC TC 56 - Dependability: , IEC 2: Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA), IEC, Geneva, Switzerland, 2006

IEC TC 56 - Dependability: IEC 61025 (2006)
IEC TC 56 - Dependability: , IEC 2: Fault Tree Analysis (FTA), IEC, Geneva, Switzerland, 2006

IEC TC 56 - Dependability: IEC 61882 (2016)
IEC TC 56 - Dependability: , IEC 2: Hazard and Operability Studies (HAZOP Studies) - Application Guide, IEC, Geneva, Switzerland, 2016

IEC TC 65/SC 65A - System aspects: IEC 61508 (2011)
IEC TC 65/SC 65A - System aspects: , IEC 2: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC, Geneva, Switzerland, 2011

ISO TC 22/SC 32 Electrical and electronic components and general system aspects: ISO 26262 (2011)
ISO TC 22/SC 32 Electrical and electronic components and general system aspects: , ISO Road Vehicles - Functional Safety, ISO, Geneva, Switzerland, 2011

ISO/TC 199 - Safety of machinery: EN ISO 13849 (2015)
ISO/TC 199 - Safety of machinery: , ISO 3: Safety of Machinery -- Safety-Related Parts of Control Systems, ISO, Geneva, Switzerland, 2015

ISO/TC 262 - Risk management: IEC 31010 (2009)
ISO/TC 262 - Risk management: , IEC 1: Risk Management -- Risk Assessment Techniques, ISO, Geneva, Switzerland, 2009

Johnson, D. M.: Review of Simulator Sickness Research (2005)
Johnson, David M.: Introduction to and Review of Simulator Sickness Research, U.S. Army Research Institute for the Behavioral and Social Sciences Research Report, Arlington, VA, USA, 2005

Kawamura, H. et al.: Highly-Responsive Acceleration Control for Nissan LEAF (2011)
Kawamura, Hiromichi; Ito, Ken; Karikomi, Takaaki; Kume, Tomohiro: Highly-Responsive Acceleration Control for the Nissan LEAF Electric Vehicle, in: Proceedings of the SAE World Congress & Exhibition 2011, SAE Technical Paper Series, SAE, 2011

Kemeny, A. et al.: DSC Europe 2016 (2016)
Kemeny, Andras; Mérienne, Frédéric; Colombet, Florent; Espié, Stéphane (Eds.) Proceedings of the Driving Simulation & Virtual Reality Conference & Exhibition Europe 2016 (DSC), 2016

Kemeny, A. et al.: DSC Europe 2017 (2017)
Kemeny, Andras; Colombet, Florent; Mérienne, Frédéric; Espié, Stéphane (Eds.) Proceedings of the Driving Simulation & Virtual Reality Conference & Exhibition Europe 2017 (DSC), 2017

Kroemer, K. H. et al.: Engineering Physiology (2010)
Kroemer, Karl H. E.; Kroemer, Hiltrud J.; Kroemer-Elbert, Katrin E.: Engineering Physiology, Springer, Berlin, Heidelberg, Germany, 2010

Maurer, M. et al.: Autonomes Fahren (2015)
Maurer, Markus; Gerdes, J. C.; Lenz, Barbara; Winner, Hermann: Autonomes Fahren, Springer Vieweg, Berlin, Heidelberg, Germany, 2015

Max Planck Institute for Biological Cybernetics: CableRobot with Passenger (2015)
Max Planck Institute for Biological Cybernetics: CableRobot with Passenger; https://tuebingen.mpg.de/en/homepage/detail/cablerobot-with-passenger-1.html, 2015, Access 11.10.2016

Murano, T. et al.: Development of High-Performance DS (2009)
Murano, Takahiko; Yonekawa, Takashi; Aga, Masami; Nagiri, Sueharu: Development of High-Performance Driving Simulator, in: SAE International Journal of Passenger Cars - Mechanical Systems (1), Issues 2, pp. 661–669, 2009

Nahon, M.; Reid, L. D.: Simulator MCA - A Designer's Perspective (1990)
Nahon, Meyer; Reid, Lloyd D.: Simulator Motion-Drive Algorithms - A Designer's Perspective, in: Journal of Guidance, Control, and Dynamics (2), Issues 13, pp. 356–362, 1990

Nieuwenhuizen, F. M.; Bülthoff, H. H.: The MPI CyberMotion Simulator (2013)
Nieuwenhuizen, Frank M.; Bülthoff, Heinrich H.: The MPI CyberMotion Simulator, in: Journal of Computing Science and Engineering (2), Issues 7, pp. 122–131, 2013

Osczevski, R.; Bluestein, M.: Wind Chill Equivalent Temperature Chart (2005)
Osczevski, Randall; Bluestein, Maurice: The New Wind Chill Equivalent Temperature Chart, in: Bulletin of the American Meteorological Society (10), Issues 86, pp. 1453–1458, 2005

Pfaffenbichler, P. C. et al.: Electric Mobility in Austria (2009)
Pfaffenbichler, Paul C.; Emmerling, Bettina; Jellinek, Reinhard; Krutak, Robin: Pre-Feasibility-Studie zu "Markteinführung Elektromobilität in Österreich", Vienna, Austria, 2009

Pfeffer, P.; Harrer, M.: Lenkungshandbuch (2011)
Pfeffer, Peter; Harrer, Manfred: Lenkungshandbuch, Vieweg+Teubner, Wiesbaden, Germany, 2011

Ploeg, J. et al.: High Performance Automatic Guided Vehicle (2002)
Ploeg, Jeroen; van der Knaap, Albert C. M.; Verburg, Dirk J.: ATS/AGV-Design, Implementation and Evaluation of a High Performance AGV, in: Proceedings of the IEEE Intelligent Vehicle Symposium 2002 (IV), IEEE, Piscataway, NJ, USA, 2002

17th SIMVEC (2014) Proceedings of the 17th Simulation und Erprobung in der Fahrzeugentwicklung (SIMVEC), VDI, Düsseldorf, Germany, 2014

SAE World Congress 2011 (2011) Proceedings of the SAE World Congress & Exhibition 2011, SAE Technical Paper Series, SAE, 2011

Reason, J. T.; Brand, J. J.: Motion Sickness (1975)
Reason, James T.; Brand, Joseph J.: Motion Sickness, Acad. Press, London, UK, 1975

Reid, L. D.; Nahon, M.: Flight Simulation MCA (1985)
Reid, Lloyd D.; Nahon, Meyer: Flight Simulation Motion-Base Drive Algorithms, UTIAS Report, MMMM, 1985

Richter, A.; Scholz, M.: The Surveyor's Guide to Automotive Simulation (2016)
Richter, Andreas; Scholz, Michael: "The Surveyor's Guide to Automotive Simulation": Development and Evaluation of Guidelines for Straight Forward Road Surveying for Driving Simulator Databases and Test Development of Driver Assistance and Automation Systems, in: Kemeny, Andras et al. (Eds.): Proceedings of the Driving Simulation & Virtual Reality Conference & Exhibition Europe 2016 (DSC), 2016

SAE: Terms Related to Automated Driving Systems (2014)
SAE: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, SAE; https://doi.org/10.4271/J3016_201401, 2014

Sato, Y. et al.: High Response Motor Nissan LEAF (2011)
Sato, Yoshinori; Ishikawa, Shigeaki; Okubo, Takahito; Abe, Makoto; Tamai, Katsunori: Development of High Response Motor and Inverter System for the Nissan LEAF Electric Vehicle, in: Proceedings of the SAE World Congress & Exhibition 2011, SAE Technical Paper Series, SAE, 2011

Schöner, H.-P.: Erprobung und Absicherung im dynamischen DS (2014)
Schöner, Hans-Peter: Erprobung und Absicherung im dynamischen Fahrsimulator, in: Proceedings of the 17th Simulation und Erprobung in der Fahrzeugentwicklung (SIMVEC), VDI, Düsseldorf, Germany, 2014

Schöner, H.-P.; Morys, B.: Dynamische DS (2015)
Schöner, Hans-Peter; Morys, Bernhard: Dynamische Fahrsimulatoren, in: Winner, Hermann (Ed.): Handbuch Fahrerassistenzsysteme, ATZ, Vieweg+Teubner, Wiesbaden, Germany, 2015

Slob, J. J.: State-of-the-Art DS (2008)
Slob, J. J.: State-of-the-Art Driving Simulators, a Literature Survey, Eindhoven, Netherlands, 2008

Slob, J. J. et al.: The Wall is the Limit (2009)
Slob, J. J.; Kuijpers, M. R. L.; Rosielle, P. C. J. N.; Steinbuch, M.: A New Approach to Linear Motion Technology: The Wall is the Limit, in: Kemeny, Andras (Ed.): Proceedings of the Driving Simulation Conference Europe 2009 (DSC), INRETS, Arcueil, France, 2009

St. Pierre, M. E.: Diss., The Effects of Latency on Simulator Sickness in a HMD (2012)
St. Pierre, Matthew E.: The Effects of 0.2 Hz Varying Latency with 20-100 ms Varying Amplitude on Simulator Sickness in a Helmet Mounted Display, Dissertation Clemson University, All DissertationsPaper 1036, TigerPrints, 2012

St. Pierre, M. E. et al.: The Effects of Latency on Simulator Sickness in a HMD (2015)
St. Pierre, Matthew E.; Banerjee, Salil; Hoover, Adam W.; Muth, Eric R.: The Effects of 0.2 Hz Varying Latency with 20-100 ms Varying Amplitude on Simulator Sickness in a Helmet Mounted Display, in: Displays, Issues 36, pp. 1–8, 2015

Stewart, D.: A Platform with Six DOF (1965)
Stewart, David: A Platform with Six Degrees of Freedom, in: ARCHIVE: Proceedings of the Institution of Mechanical Engineers 1847-1982 (vols 1-196) (1965), Issues 180, pp. 371–386, 1965

Teufel, H. et al.: MPI Motion Simulator (2007)
Teufel, Harald; Nusseck, Hans-Günther; Beykirch, Karl; Butler, John; Kerger, Michael; Bülthoff, Heinrich: MPI Motion Simulator: Development and Analysis of a Novel Motion Simulator, in: Proceedings of the AIAA Modeling and Simulation Technologies Conference and Exhibit 2007, AIAA, 2007

Tischer, W.; Prokop, G.: Selbstfahrender, hochdynamischer Fahrsimulator (2014)
Tischer, Wolfgang; Prokop, Günther: Selbstfahrender, hochdynamischer Fahrsimulator, Amst-Systemtechnik Gmbh, Technische Universität Dresden, Patent WO2014198861 A1, Patent application number: PCT/EP2014/062304, 2014

TU Delft: Validation Methodology for Fault-Tolerant ADAS (2014)
TU Delft: Validation Methodology for Fault-Tolerant Advanced Driver Assistance Systems; http://www.dcsc.tudelft.nl/Research/Old/project_og_bds_mv.html, 2014, Access 21.10.2016

Tüschen, T.: Diplomarbeit, MCA für einen WMDS (2013)
Tüschen, Thomas: Konzeptionierung und Aufbau eines Motion-Cueing Algorithmus für einen selbstfahrenden Fahrsimulator, Diplomarbeit
Technische Universität Dresden, Dresden, Germany, 2013

Tüschen, T. et al.: Suspensions Design of a WMDS (2016)
Tüschen, Thomas; Kocksch, Felix; Beitelschmidt, Denise; Prokop, Günther: "auto.mobile-driving simulator" – Suspensions Design of a Wheel-Based Driving Simulator, in: Pfeffer, Peter (Ed.): Proceedings of the 7th International Munich Chassis Symposium (chassis.tech plus), Springer, Wiesbaden, Germany, 2016

Tüschen, T.; Prokop, G.: Development of a Highly Dynamic DS (2013)
Tüschen, Thomas; Prokop, Günther: Development of a Highly Dynamic Driving Simulator, in: Proceedings of the 16th ITI-Symposium, 2013

Tüschen, T.; Prokop, G.: System Design of a Highly Dynamic DS (2014)
Tüschen, Thomas; Prokop, Günther: System Design of a Highly Dynamic Driving Simulator by Means of a FMU Co-Simulation, in: Proceedings of the 17th ITI-Symposium, 2014

UNITEK Industrie Elektronik GmbH: Manual Bamocar-D3 (2017)
UNITEK Industrie Elektronik GmbH: Manual Bamocar-D3; https://www.unitek-industrie-elektronik.de/menu-bamocar-eng/menu-bamocar-pg-d3-eng, 2017, Access 16.01.2018

University of Leeds: University of Leeds DS (2016)
University of Leeds: UoLDS: Facility; http://www.uolds.leeds.ac.uk/facility/, 2016, Access 11.10.2016

van der Meulen, S. H.: Validation of Moving Base Simulation Model (2004)
van der Meulen, S. H.: Validation, Improvement and Analysis of Moving Base Simulation Model, DCT rapporten Vol. 2005.056, Eindhoven, Netherlands, 2004

van der Slot, A. et al.: Integrated Fuels and Vehicles Roadmap to 2030+ (2016)
van der Slot, Arnoud; Schlick, Thomas; Pfeiffer, Walter; Baum, Markus: Integrated Fuels and Vehicles Roadmap to 2030+, Munich, Germany, 2016

VI-grade: VI-grade DiM (2017)
VI-grade: DRIVER-IN-MOTION - Driving Simulation Solution | VI-grade; https://www.driverinmotion.com/, 2017, Access 06.12.2017

VTI: VTI's simulator facilities
VTI: VTI's Simulator Facilities; http://www.vti.se/en/research-areas/vehicle-technology/vtis-driving-simulators/, Access 11.10.2016

Wagner, P.: Master's thesis, Aufbau und Inbetriebnahme eines WMDS (2013)
Wagner, Paul: Aufbau und Inbetriebnahme eines selbstfahrenden Fahrsimulatorprüfstands, Master's thesis
Technische Universität Darmstadt, Darmstadt, Germany, 2013

Wagner, P. et al.: Conception and Design of Mobile Driving Simulators (2014)
Wagner, Paul; Betz, Alexander; Winner, Hermann: Conception and Design of Mobile Driving Simulators, in: Proceedings of the ASME International Design Engineering Technical Conferences and Computers and Information in Engineering Conference 2014 (IDETC/CIE), ASME, New York, NY, USA, 2014

Wagner, P. et al.: Potentials and Limitations of Hexapods in WMDS (2015)
Wagner, Paul; Davoodi, Aschkan; Scheibe, Thomas; Albrecht, Torben; Winner, Hermann: Potentials and Limitations of Hexapods in Wheeled Mobile Driving Simulators, in: Bülthoff, Heinrich; Kemeny, Andras; Pretto, Paolo (Eds.): Proceedings of the Driving Simulation Conference & Exhibition Europe 2015 (DSC), Tübingen, Germany, 2015

Wagner, P. et al.: Power, Energy, and Latency Test Drives with MORPHEUS (2017)
Wagner, Paul; Zöller, Chris; Albrecht, Torben; Winner, Hermann: Power, Energy, and Latency Test Drives with the Wheeled Mobile Driving Simulator Prototype MORPHEUS, in: Kemeny, Andras et al. (Eds.): Proceedings of the Driving Simulation & Virtual Reality Conference & Exhibition Europe 2017 (DSC), 2017

Wentink, M. et al.: Design and Evaluation of MCA for Desdemona Simulator (2005)
Wentink, Mark; Bles, Wim; Hosman, Ruud; Mayrhofer, Michael: Design and Evaluation of Spherical Washout Algorithm for Desdemona Simulator, in: Proceedings of the AIAA Modeling and Simulation Technologies Conference and Exhibit 2005, AIAA, 2005

Wildzunas, R. M. et al.: Visual Display Delay Effects on Pilot Performance (1996)
Wildzunas, Robert M.; Barron, Terry L.; Wiley, Roger W.: Visual Display Delay Effects on Pilot Performance, in: Aviation, Space, and Environmental Medicine (3), Issues 67, pp. 214–221, 1996

Winner, H.: Handbuch Fahrerassistenzsysteme (2015)
Winner, Hermann (Ed.) Handbuch Fahrerassistenzsysteme, ATZ, Vieweg+Teubner, Wiesbaden, Germany, 2015

Zeeb, E.: Daimler's New Full-Scale, High-Dynamic DS (2010)
Zeeb, Eberhard: Daimler's New Full-Scale, High-Dynamic Driving Simulator – A Technical Overview, in: Kemeny, Andras; Mérienne, Frédéric; Espié, Stéphane (Eds.): Proceedings of the Driving Simulation Conference Europe 2010 (DSC), 2010

Zöller, C.: Master's thesis, Implementierung und Parametrierung eines Reifenmodells für WMDS (2014)
Zöller, Chris: Implementierung eines Fahrdynamiksimulationstauglichen Modells des Bandagenreifens des WMDS sowie Identifikation der relevanten Parameter, Master's thesis
Technische Universität Darmstadt, Darmstadt, Germany, 2014

Zöller, C. et al.: Tire Concept Investigation for WMDS (2016)
Zöller, Chris; Wagner, Paul; Winner, Hermann: Tire Concept Investigation for Wheeled Mobile Driving Simulators, in: Kemeny, Andras et al. (Eds.): Proceedings of the Driving Simulation & Virtual Reality Conference & Exhibition Europe 2016 (DSC), 2016

Zöller, C. et al.: Tires and Vertical Dynamics of WMDS (2017)

Zöller, Chris; Wagner, Paul; Winner, Hermann: Tires and Vertical Dynamics of Wheeled Mobile Driving Simulators, in: Transportation Research Part F: Traffic Psychology and Behaviour, 2017

Publications

Betz, A.; Butry, A.; Junietz, P.; Wagner, P.; Winner, H.: Driving Dynamics Control of a Wheeled Mobile Driving Simulator Utilizing an Omnidirectional Motion Base for Urban Traffic Simulation. In *Proceedings of the Future Active Safety Technology toward zero-traffic-accident – FAST-zero*, September 22-26, Nagoya, Japan, 2013

Wagner, P.; Betz, A.; Winner, H.: Conception and Design of Mobile Driving Simulators. In *Proceedings of the ASME 2014 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference – IDETC/CIE*, August 17-20, Buffalo, NY, USA, 2014.

Betz, A.; Wagner, P.; Albrecht, T.; Winner, H.: Development and Validation of a Safety Architecture of a Wheeled Mobile Driving Simulator. In *Proceedings of the Driving Simulation Conference Europe – DSC*, September 4-5, Paris, France, 2014.

Betz, A.; Wagner, P.; Scheibe, T.; Winner, H.: Konzeptanalyse und Erprobung eines selbstfahrenden Fahrsimulators für die Simulation von Stadtverkehr, In *Proceedings of the 16th Simulation und Erprobung in der Fahrzeugentwicklung – SIMVEC*, November 18-19, Baden-Baden, Germany, 2014.

Wagner, P.; Davoodi, A.; Scheibe, T.; Albrecht, T.; Betz, A.; Winner, H.: Potentials and Limitations of Hexapods in Wheeled Mobile Driving Simulators. In *Proceedings of the Driving Simulation Conference & Exhibition Europe –- DSC*, September 16-18, Tübingen, Germany, 2015.

Schneider, J.; Wagner, P.; Winner, H.: Situational Adaptive Chassis: Where are the Limits?. In *Proceedings of the 24th Aachener Kolloquium –- AC*, October 5-7, Aachen, Germany, 2015.

Wagner, P.; Winner, H.: MiniMax-Projekt – Fahrwerkskonzept für urbanen Straßenverkehr. *Automobiltechnische Zeitschrift –- ATZ* 118(6): 26–33, 2016.

Wagner, P.; Zöller, C..; Winner, H.: Safety Analysis for Wheeled Mobile Driving Simulators. In *Proceedings of the Driving Simulation Conference & Virtual Reality Conference & Exhibition Europe –- DSC*, September 7-9, Paris, France, 2016.

Zöller, C.; Wagner, P.; Winner, H.: Tire Concept Investigation for Wheeled Mobile Driving Simulators. In *Proceedings of the Driving Simulation Conference & Virtual Reality Conference & Exhibition Europe –- DSC*, September 7-9, Paris, France, 2016.

Kalbfleisch, J.; Wagner, P.; Winner, H.: MiniMax – a Situational and Geometrical Adaptive Chassis: Driving Safety AND Space Efficiency. In *Proceedings of the 13th International Symposium on Advanced Vehicle Control -– AVEC*, September 13-16, Munich, Germany, 2016.

Wagner, P.; Zöller, C.; Albrecht, T.; Winner, H.: Power, Energy, and Latency Test Drives with the Wheeled Mobile Driving Simulator Prototype MORPHEUS. In *Proceedings of the Driving Simulation Conference & Virtual Reality Conference & Exhibition Europe -– DSC*, September 6-8, Stuttgart, Germany, 2017.

Zöller, C.; Wagner, P.; Winner, H.: Tire Concept Investigation for Wheeled Mobile Driving Simulators. *Transportation Research Part F: Traffic Psychology and Behaviour*, Special Issue Driving Simulation, 2017.

Supervised Students' Thesis

Li, X., Wang, C., Lu, F., Yu, L., Li, Z.: Konzeption eines Prüfstands zur Bestimmung der Abhängigkeit von Reifenschräglauf und Seitenkraft bei Bandagereifen, Advanced Design Project Nr. 50/14, 2014.

Kettmann, N.: Menschliche Wahrnehmungsschwellen für Bewegung in der Fahrsimulation, Forschungsseminar Nr. 105/14, 2014.

Drachenberg, A.: Implementierung eines Bandagereifenmodells des selbstfahrenden Fahrsimulators in IPG CarMaker, Bachelorthesis Nr. 1178/14, 2014.

Prinz, J.: Putting into Operation of Wheeled Mobile Driving Simulator Including its Safety System, International Research Experience, 2014.

Scheibe, T.: Untersuchung der mechanischen Kopplung im selbstfahrenden Fahrsimulator sowie Identifikation von Reifenparametern, Masterthesis Nr. 546/14, 2014.

Albrecht, T.: Implementierung und Parametrisierung eines Hexapod in den Motion Cueing Algorithmus eines selbstfahrenden Fahrsimulators, Bachelorthesis Nr. 1200/14, 2014.

Davoodi, A.: Stillstandsvermeidung der Räder im selbstfahrenden Fahrsimulator, Bachelorthesis Nr. 1204/14, 2014.

Schneider, J.: Untersuchung der fahrdynamischen Auswirkungen eines situativ anpassbaren Fahrwerks auf die Fahrstabilität, Masterthesis Nr. 548/14, 2014.

Zöller, C.: Implementierung eines Fahrdynamiksimulationstauglichen Modells des Bandagenreifens des WMDS sowie Identifikation der relevanten Parameter, Masterthesis Nr. 557/14, 2014.

Zhang, Z.: Modelling and Design of a Safety System for a Wheeled Mobile Driving Simulator, International Research Experience, 2015.

Bilgic Istoc, S.: Einbindung und Validierung von Testmanövern in den selbstfahrenden Fahrsimulator, Masterthesis Nr. 578/15, 2015.

Kalbfleisch, J.: Konzeptauswahl für ein situativ anpassbares Fahrwerk, Masterthesis Nr. 580/15, 2015.

Yang, J.: Überarbeitung und Optimierung des Motion Cueing Algorithmus eines selbstfahrenden Fahrsimulators, Masterthesis Nr. 581/15, 2015.

Butry, A.: Analyse und Weiterentwicklung der Ansteueralgorithmen eines Fahrsimulators, Masterthesis Nr. 582/15, 2015.

Schneider, J.; Seyfried, S.; Brötz, N.; Alles, J.; Mrosek, M.; Rösner, A.: Weiterentwicklung eines automatisierten und Smartphone-basierten Aufzeichnungssystem von Fahrdaten, Advanced Design Project Nr. 66/15, 2015.

Forster, P.: Entwurf eines hochdynamischen und überaktuierten Fahrzeugs zum präzisen Handling von Objekten, Diplomarbeit Nr. 595/15, 2015.

Xu, C.: Analyse von Umfeldsensorik für selbstfahrende Roboter, Forschungsseminar Nr. 146/15, 2015.

Senol, S.: Analyse von Sicherheitsmechanismen für selbstfahrende Roboter, Forschungsseminar Nr. 147/15, 2015.

Steier. J.: Erweiterung der Bewegungsregelung eines selbstfahrenden Fahrsimulators, Masterthesis Nr. 598/15, 2015.

Lutwitzi, M.: Entwurf eines Konzepts für eine Umfelderkennung für selbstfahrende Fahrsimulatoren, Bachelorthesis Nr. 1272/16, 2016.

Glatzki, F.: Untersuchung des Einflusses einer Trajektorienüberlagerung auf den Lenkleistungsbedarf eines selbstfahrenden Fahrsimulators, Bachelorthesis Nr. 1273/16, 2016.

Bonakdar, F.: Verbesserung der Bewegungsregelung eines selbstfahrenden Fahrsimulators, Bachelorthesis Nr. 1275/16, 2016.

Titze, J.: Recherche und Vergleich von Personal Electric Vehicles und geometrisch verstellbaren Fahrwerken, Studienarbeit Nr. 1276/16, 2016.

Luft, A.: Konzeption eines skalierten Personal Electric Vehicle mit aktiver Spurweite- und Schwerpunktverstellung, Masterthesis Nr. 618/16, 2016.

Betschinske, D.: Untersuchung von Methoden zur Verringerung des Lenkleistungsbedarfs des selbstfahrenden Fahrsimulators, Bachelorthesis Nr. 1287/16, 2016.

Perschbacher, R.: Untersuchung der Eignung eines Hexapods zur Maskierung von Störeinflüssen aus der Lenkung an einem selbstfahrenden Fahrsimulator, Bachelorthesis Nr. 1288/17, 2017.

Hein, E.; Lamrabet, Y.; Niess, S.; Weiher, M.: Entwicklung des selbstfahrenden Fahrsimulators MORPHEUS 2.0, Advanced Design Project Nr. 100/17, 2017.